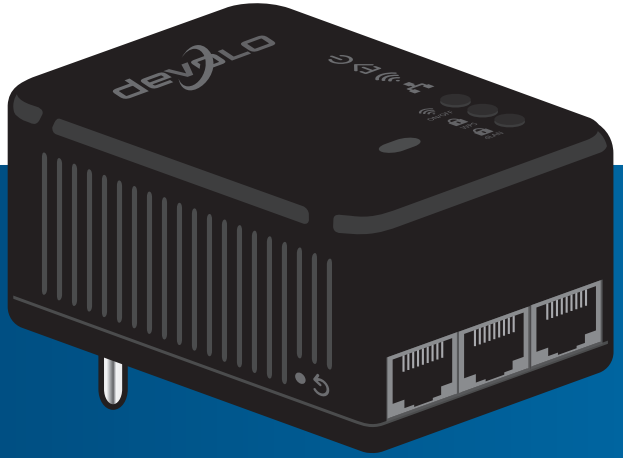
dLAN®

200 AVpro Wireless N



The Network Innovation

devolo dLAN® 200 AVpro Wireless N

© 2012 devolo AG Aachen (Germany)

While the information in this manual has been compiled with great care, it may not be deemed an assurance of product characteristics. devolo shall be liable only to the degree specified in the terms of sale and delivery.

The reproduction and distribution of the documentation and software supplied with this product and the use of its contents is subject to written authorization from devolo. We reserve the right to make any alterations that arise as the result of technical development.

Trademarks

HomePlug® is a registered trademark of HomePlug Powerline Alliance.

Linux® is a registered trademark of Linus Torvalds.

Ubuntu®is a registered trademark of Canonical Ltd.

Mac® and Mac OS X® are registered trademarks of Apple Computer, Inc.

Windows® and Microsoft® are registered trademarks of Microsoft, Corp.

Wi-Fi®, Wi-Fi Protected Access™, WPA™, WPA2™ and Wi-Fi Protected Setup™ are registered trademarks of the Wi-Fi Alliance®.

devolo, dLAN®, Vianect® and the devolo logo are registered trademarks of devolo AG.

The firmware package from devolo contains files which are covered by different licenses, in particular under devolo proprietary license and under open source license (GNU General Public License, GNU Lesser General Public License or FreeBSD License). The source code which is available for Open Source distribution can be requested in writing from gpl@devolo.de.

All other names mentioned may be trademarks or registered trademarks of their respective owners. Subject to change without notice. No liability for technical errors or omissions.

devolo AG

Charlottenburger Allee 60

52068 Aachen

Germany

www.devolo.com

Aachen, April 2012

Content

1 Preface 5
1.1 Thank you for placing your trust in this devolo product 5
1.1.1 About this manual 5
1.2 CE conformity 6

2 Introduction 7
2.1 What exactly is dLAN? 7
2.2 What is WLAN? 7
2.3 What is VLAN? 7
2.4 dLAN 200 AVpro Wireless N 8
2.5 Sample applications 9
2.5.1 dLAN 200 AVpro Wireless N as a WLAN access point 9
2.5.2 dLAN 200 AVpro Wireless N as a WLAN client 11
2.5.3 dLAN 200 AVpro Wireless N and VLAN 12

3 Initial use 17
3.1 Package contents 18
3.2 System requirements 18
3.3 Functions 19
3.3.1 Control lamps 19
3.3.2 Buttons 20
3.3.3 Network jacks 21
3.3.4 WLAN antennas 22
3.4 Connecting the dLAN 200 AVpro Wireless N 22
3.4.1 Software for Windows 23

4 Network configuration 25
4.1 Calling up the built-in configuration interface 25
4.2 Menu description 25
4.3 Status overview 26

4.3.1 dLAN status 28
4.3.2 WLAN status 28
4.4 Device configuration 29
4.4.1 Security 29
4.4.2 Network settings 33
4.4.3 dLAN settings 35
4.4.4 Time server 36
4.5 Disabling WLAN configuration 37
4.6 WLAN configuration as access point 38
4.6.1 WLAN basic settings 40
4.6.2 Security settings for the access point 43
4.6.3 Wi-Fi Protected Setup (WPS) 48
4.7 WLAN configuration as client 50
4.7.1 Security settings for the WLAN client 53
4.8 VLAN configuration 55
4.8.1 Create VLAN 57
4.8.2 Overview of configured VLANs 57
4.8.3 VLAN port settings 58
4.9 Management 60
4.9.1 Resetting the configuration 61
4.9.2 Saving a configuration file 62
4.9.3 Restoring a configuration 63
4.9.4 Update firmware 63

5 dLAN network 65
5.1 Security in the dLAN 65
5.2 dLAN AVpro network encryption at the touch of a button 65
5.3 dLAN AVpro manager for Windows 69

6 Appendix 71
6.1 Important safety instructions 71
6.2 Disposal of old devices 72
6.3 Warranty conditions 72

1 Preface

1.1 Thank you for placing your trust in this devolo product

devolo dLAN business solutions are a favourably priced option for using the power grid infrastructure in a building to establish a broadband IP network. The advantage this brings is obvious: no new cables have to be laid – expenditure and costs remain low.

The dLAN 200 AVpro Wireless N is devolo's innovative access point for mobile as well as stationary network devices in a professional environment. Positioning anywhere in a building is possible due to the flexibility of dLAN networking over an existing power line: even areas without a network connection are perfectly integrated this way.

1.1.1 About this manual

After an introduction to "dLAN", "WLAN" and "VLAN" basics in **Chapter 2**, **Chapter 3** will cover successfully setting up your dLAN 200 AVpro Wireless N. **Chapter 4** describes in detail the setting options of the built-in configuration interface and thereby also access to the dLAN, VLAN and WLAN. For information on configuring the dLAN network, please see **Chapter 5**. Information about product safety and environmental compatibility of the device and our warranty terms can be found in **Chapter 6** and conclude the manual.

You can find the technical data for the dLAN 200 AVpro Wireless N in the product information sheet on the enclosed product CD.

Description of the symbols

Here we briefly describe the meaning of the symbols used in this manual.

Very important note. Failure to observe this note may result in damage.

Important note that should be observed.

Additional information, background material and configuration tips for your device.

If you have any further ideas or suggestions related to our products, please don't hesitate to contact us at support@devolo.com!

devolo on the Internet

For detailed information on our products, visit www.devolo.com.

The download area provides you not only with product descriptions and documentation, but also updates of devolo software and your device's firmware. We especially recommend the descriptions on the topic of "dLAN networking" that contain a wealth of interesting background information.

1.2 CE conformity

CE 2150

This product complies with the technical requirements of the directive 1999/5/EC (R&TTE) and the other relevant provisions of the FTEG, and it is designed for use in the EU and Switzerland. The product is class A equipment. Class A devices may cause interference when used in residential environments.

"99/05/CE" (R&TTE directive) is a directive similar to the EMC directive. It applies to radio equipment and telecommunication terminal equipment.Observance of these directives is verified by the use of harmonized European norms.
For the CE declaration for this product, refer to the accompanying product CD under **CE**.

2 Introduction

dLAN is an intelligent, secure technology that lets you set up a home network easily, quickly and economically via your household electrical wiring, without the need for complex and expensive dedicated cabling. The available performance and effort required for the installation also compares favourably to traditional methods.

2.1 What exactly is dLAN?

dLAN (**d**irect **L**ocal **A**rea **N**etwork) uses the household power grid to transfer data between computers equipped with suitable adapters and other network components. As a result, any power outlet can be used as a network access point. The data is modulated prior to transfer and sent as a signal via household power lines. State-of-the-art technology ensures that the power and data networks do not interfere with one another. Networking via dLAN is fast and secure. The data is encrypted using a key to prevent easy interception by third parties.

2.2 What is WLAN?

WLAN (**W**ireless **L**ocal **A**rea **N**etwork) refers to the use of radio technology to network computers and other devices. While it is possible to wirelessly connect computers in pairs (peer-to-peer, p2p), a central access point is required to set up a network of multiple devices. Such access points are frequently combined in a single device with modems for Internet access and routers to manage network traffic.

The wireless network established by an access point using a specific channel (from 1 to 13) and name (SSID) has a limited range. The range of the access point, which is also known as a "radio cell", is impeded by building walls. In some cases, stable connections are often only possible between WLAN devices within a single room.

As it is not possible to rely on hardware such as network cables (in a LAN) or household wiring (in a dLAN) to control access to a WLAN, wireless networking naturally presents special security challenges. WLANs therefore use a number of security measures, such as a concealed network name, data encryption and access control via the MAC addresses of the network adapters.

2.3 What is VLAN?

A **VLAN** (**V**irtual **L**ocal **A**rea **N**etwork) is a logical, self-enclosed, local network—unlike a physical (switched) network. **VLANs** divide **physical** networks into multi-

ple **logical networks that are independent** of each other and can be better protected against intrusion and interception than switched networks. They optimise data distribution and relieve the burden on overloaded networks.

Using VLANs prevents the need for complicated physical wiring. This gives you greater spatial flexibility and saves you having to purchase multiple costly individual devices (e.g. router, switches).

The allocation to a VLAN can take place statically via port assignment, via special marks on the data packets (tagged packets) or dynamically, e.g. through MAC and IP addresses, TCP and UDP ports or higher protocols.

2.4 dLAN 200 AVpro Wireless N

- Innovative access point for network-compatible terminal devices; whether dLAN, WLAN or classic network cable: every device can be connected!
- The dLAN powerline technology uses the internal power line and thus enables flexible positioning of the dLAN 200 AVpro Wireless N everywhere in the building.
- Areas without network cables are integrated perfectly; alternatively, an existing network is ideally extended.
- Developed for use in businesses; already tried and tested in a multitude of sectors such as hospitality, offices and production.
- Ideal for all public areas: an integrated Kensington Lock reliably protects the adapter from theft.
- Easy set-up of WLAN zones (WLAN access points and wireless hotspots) with support of the WLAN IEEE 802.11n high-speed standard.
- Separation of user groups and granular access control through Multi SSID and VLAN.
- Ideal as a comprehensive, fast and stable network solution or for support of existing network infrastructure.
- 200 Mbps (gross) connection for fast data transmission via dLAN, 300 Mbps (gross) in WLAN operation (IEEE 802.11n standard).
- Professional WLAN security management with support for WPA, WPA2 and WPA2 Enterprise.
- Optimal dLAN security with a 128-bit AES key.
- Remote management via the devolo dLAN AVpro manager software.
- Simple configuration via web interface.
- Optimal modification of the adapter for any usage scenario through network ports that can be disabled and the deactivation of the function buttons on the adapter.

- WLAN time control with configurable usage times.
- Two internal WLAN antennas; MIMO technology for the best transmission and reception performance.

2.5 Sample applications

2.5.1 dLAN 200 AVpro Wireless N as a WLAN access point

By default, the dLAN 200 AVpro Wireless N is configured as a WLAN access point and makes the dLAN network connected via the mains outlet available wirelessly to other client devices, such as laptops, IP radios or IP telephones. This is particularly practical if not all client stations are within range of a WLAN access point, for example because concrete walls disrupt the signal. With dLAN various rooms can be easily connected via the mains supply. And using the dLAN 200 AVpro Wireless N, every mains outlet can be turned quickly and easily into a WLAN connection with excellent reception quality.

The following illustration shows how the Internet connection is set up using the dLAN 200 AVpro Wireless N and a router, and how the connection within the network is set up using additional dLAN AVpro devices.

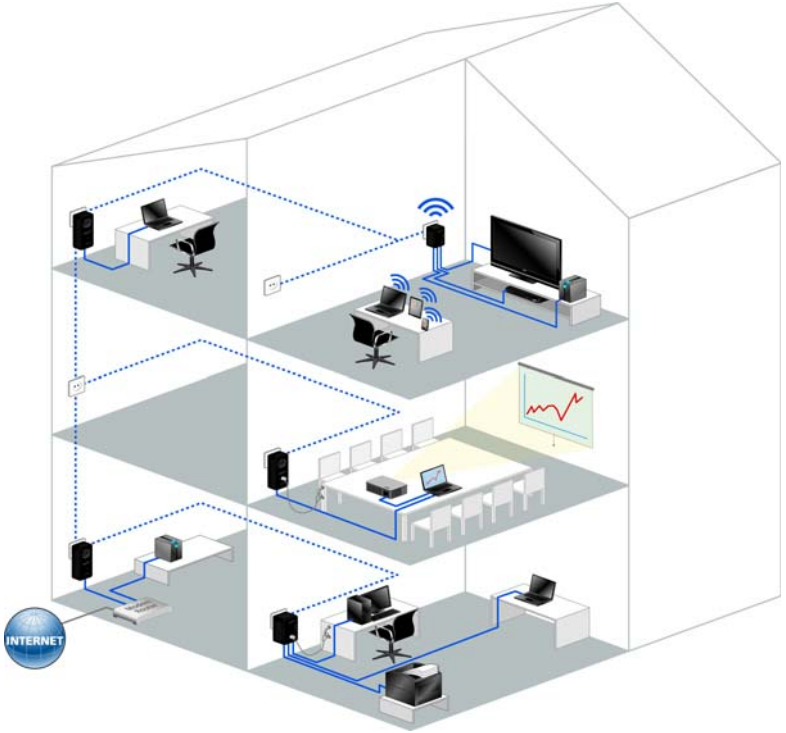


Fig. 1

2.5.2 dLAN 200 AVpro Wireless N as a WLAN client

Alternatively, the dLAN 200 AVpro Wireless N can also be configured as a WLAN client. In this case, the adapter connects the WLAN network with the devices in the dLAN network. This is especially practical if network access is not possible either via dLAN or via Ethernet wiring.

The following illustration describes how the dLAN 200 AVpro Wireless N connects multiple computers in the dLAN network wirelessly using an existing router in another network, which, in turn, provides access to the Internet via Ethernet.

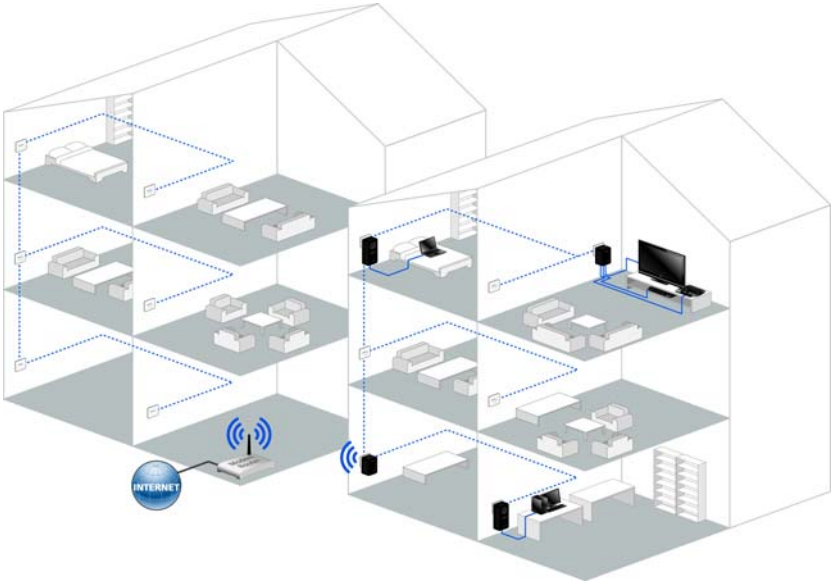


Fig. 2

2.5.3 dLAN 200 AVpro Wireless N and VLAN

Using the VLAN function, the dLAN 200 AVpro Wireless N is now also capable of setting up complex networks in a more secure and structured manner. The following illustration shows three separate VLAN networks, within which data are transmitted via dLAN or WLAN using the respective dLAN 200 AVpro Wireless N.

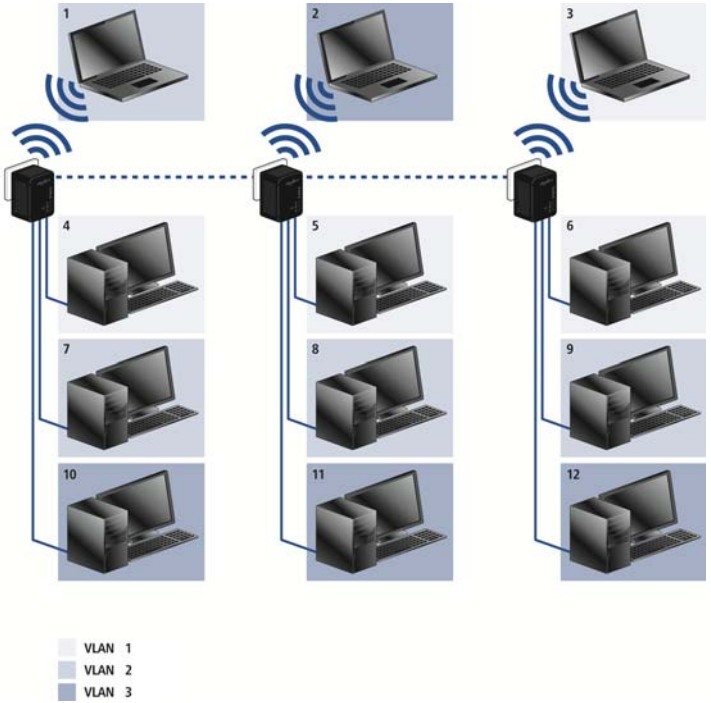


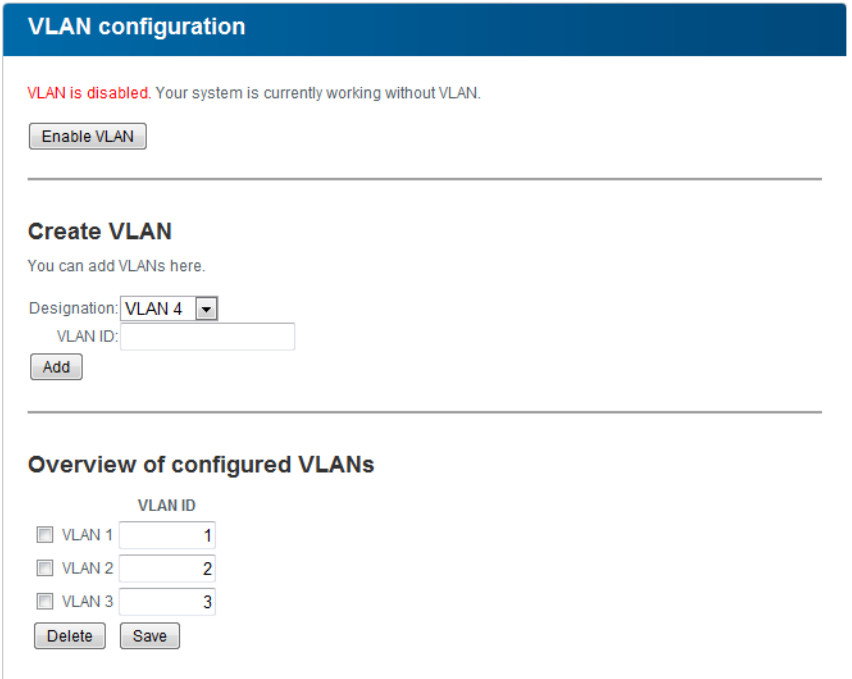
Fig. 3

This example involves three port-based VLANs (colour-coded):

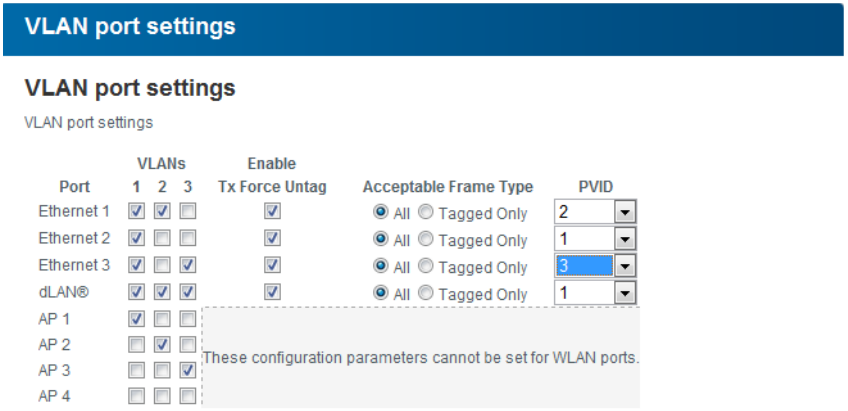
- VLAN group one (PCs 1, 7, 8, 9) e.g. at Ethernet port two
- VLAN group two (PCs 2, 10, 11, 12) e.g. at Ethernet port one
- VLAN group three (PCs 3, 4, 5, 6) e.g. at Ethernet port three
- One WLAN is assigned to each VLAN group.

The configuration of the networking example can have the following appearance:

① Under **VLAN configuration enable** the **VLAN** function and create the desired VLANs with a corresponding VLAN ID.


VLAN configuration
VLAN is disabled. Your system is currently working without VLAN.
Enable VLAN
Create VLAN
You can add VLANs here.
Designation: VLAN 4
VLAN ID:
Add
Overview of configured VLANs
VLAN ID
VLAN 1 1
VLAN 2 2
VLAN 3 3
Delete
Save

② Then under **VLAN port settings** define the assignment of the port and its behaviour.



You can find a detailed functional description for the VLAN configuration under **4.8 VLAN configuration**.

3 Initial use

This chapter covers everything you need to know to set up your dLAN 200 AVpro Wireless N. It will explain connecting the device and its functions. We will also briefly introduce the included devolo software and then guide you through its installation.

3.1 Package contents

Please ensure that the delivery is complete before beginning with the installation of your dLAN 200 AVpro Wireless N.

- **Single Kit**:
  - dLAN 200 AVpro Wireless N
  - Hard copy of installation guide
  - CD containing software and online documentation

or

- **Starter Kit**:
  - dLAN 200 AVpro Wireless N
  - dLAN 200 AVpro WP II
  - Network cable
  - Hard copy of installation guide
  - CD containing software and online documentation

devolo AG reserves the right to change the package contents without prior notice.

3.2 System requirements

- **Operating systems**: Windows XP (32-bit), Windows Vista Home Premium (32-bit/64-bit), Windows 7 Home Premium (32-bit/64-bit), Linux (Ubuntu), Mac OS X and all operating systems with network support
- **Network connection**

Please note that your computer or other device must feature a network adapter with a network port.

To set up a dLAN AVpro network, you need at least two dLAN AVpro devices (200 Mbps or 500 Mbps).

3.3 Functions

The dLAN 200 AVpro Wireless N has the following elements:

3.3.1 Control lamps

Power

Green: Lights up when the dLAN 200 AVpro Wireless N is operational.

dLAN

Green: The network connection is suitable for HD video streaming; flashes when data is being transmitted.

Orange: The network connection is suitable for SD video streaming and online gaming; flashes when data is being transmitted.

Red: The network connection is suitable for simple data transfer and Internet access; flashes when data is being transmitted.

WLAN

Green: Lit steady when a connection to the WLAN network exists; flashes when data is being transmitted.

Ethernet

Green: Lit steady when a connection to the Ethernet network exists; flashes when data is being transmitted.

3.3.2 Buttons

All buttons can be enabled or disabled on the configuration interface.

ON/OFF

Use the ON/OFF button to switch the **WLAN** function on or off.

Make sure that the WLAN function in the factory defaults is enabled and the WLAN encryption is set to WPA2. The default WLAN key is the security ID of the dLAN 200 AVpro Wireless N. You will find the 16-character security ID on the label on the back of the housing.

WPS

With the WPS (**W**i-Fi **P**rotected **S**etup) encryption button, you secure your WLAN network at the touch of a button.

WPS is one of the encryption standards developed by the Wi-Fi Alliance for increasing security in a WLAN home network. The objective of WPS is to make it easier to add devices to an existing network. For more detailed information, refer to Chapter **4.6.3 Wi-Fi Protected Setup (WPS)**.

dLAN

Via the dLAN encryption button, you secure your dLAN network at the touch of a button:

- To encrypt your dLAN AVpro network individually, press **each encryption button** on the connected devices for approx. **1 second** – within 2 minutes.
- To remove a dLAN AVpro device from your network, press the **encryption button** of the corresponding device **for at least 10 seconds**.

Reset

The **Reset** button (on the side of the housing) has two different functions:

- **The device restarts** if you press the Reset button **for less than 10 seconds**.
- To change the configuration of the dLAN 200 AVpro Wireless N back to the **factory defaults**, press the Reset button **for more than 10 seconds**. Keep in mind that all settings that have already been configured will be lost!

The reset button can be pressed using the tip of a ball-point pen.

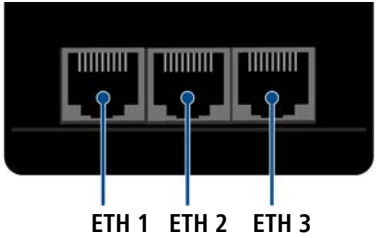
Kensington Lock

The dLAN 200 AVpro Wireless N has a slot for attaching a Kensington Lock on the front panel of the housing. A Kensington Lock is antitheft protection for portable hardware.

3.3.3 Network jacks

The three LAN ports can be used to connect computers or other network devices to the

dLAN 200 AVpro Wireless N via commercially available network cables.



3.3.4 WLAN antennas

The internal WLAN antennas are for connecting to other network devices wirelessly.

3.4 Connecting the dLAN 200 AVpro Wireless N

This section describes how to connect your dLAN 200 AVpro Wireless N to a computer or other network device.

① Use a network cable to connect the dLAN 200 AVpro Wireless N to the network port of your running computer or other network device.

② Plug the dLAN 200 AVpro Wireless N into a wall socket.

The power outlet should be in range of the connected network device.
The dLAN 200 AVpro Wireless N and the network device should be easily accessible.
To switch off the dLAN 200 AVpro Wireless N or disconnect it from the mains supply, pull the power plug out of the power outlet.

③ As soon as at least one other dLAN AV adapter has been connected and plugged into the mains supply, a dLAN network is set up. You can use devolo dLAN AVpro manager, the encryption button **or** enter the dLAN password on the configuration interface to secure your dLAN network from unauthorised access. For information on how to proceed, please read further in Chapter **4.4 Device configuration** and/or Chapter **5 dLAN network**.

For detailed information about connecting other devolo dLAN adapters, visit our website: www.devolo.com.

④ In order to be able to configure the **WLAN network**, first install the dLAN 200 AVpro Wireless N software as described in the following chapter.

3.4.1 Software for Windows

The installation wizard installs the adapter's configuration software as well as the devolo dLAN AVpro manager and the associated manual on the Windows operating system.

- In addition to the individual encryption of your dLAN network, **devolo dLAN AVpro manager** offers other expanded dLAN functions.
- Via the **configuration interface** of your **dLAN 200 AVpro Wireless N**, you can configure your WLAN network (et al.).

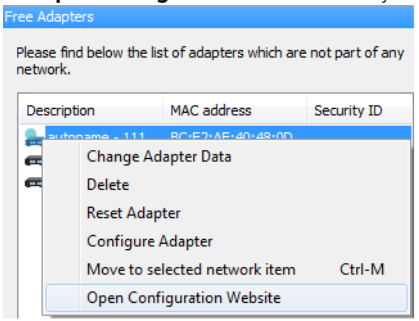
To install the software, insert the included CD-ROM in the CD drive of your computer. During the installation process, you will be given the choice of installing all software components ('Standard installation') or selecting individual ones ('Custom installation'). Then you will find the link to the configuration interface as well as the installed devolo dLAN AVpro manager and the corresponding manual in the program group **Start ⇨ All Programs ⇨ devolo**.

4 Network configuration

The dLAN 200 AVpro Wireless N has a built-in configuration interface that can be called up using a standard web browser. All settings for operating the device can be modified here.

4.1 Calling up the built-in configuration interface

You will arrive at the built-in online configuration interface of the dLAN 200 AVpro Wireless N by using the dLAN AVpro manager program under **Start ⇨ All Programs ⇨ devolo ⇨ dLAN AVpro manager**. Call up the context menu of the dLAN 200 AVpro Wireless N (right mouse button on the adapter) and click to select the **Open Configuration Website** entry.



Then the program determines the current IP address and starts the configuration in the web browser.

By default, you will come directly to the configuration interface. However, if a login password was set via the option **Device configuration ⇨ Security**, *you have to enter this first. Read more about this under* **4.4.1 Security**.

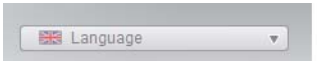
4.2 Menu description

All menu functions are described in the corresponding interface as well as in the associated chapter in the manual. The sequence of the description in the manual follows the structure of the menu.

Click **Save** to save the settings of the respective area of the configuration interface.

Click **Back** to leave the respective area of the configuration interface.

Select the desired language in the language selection list.

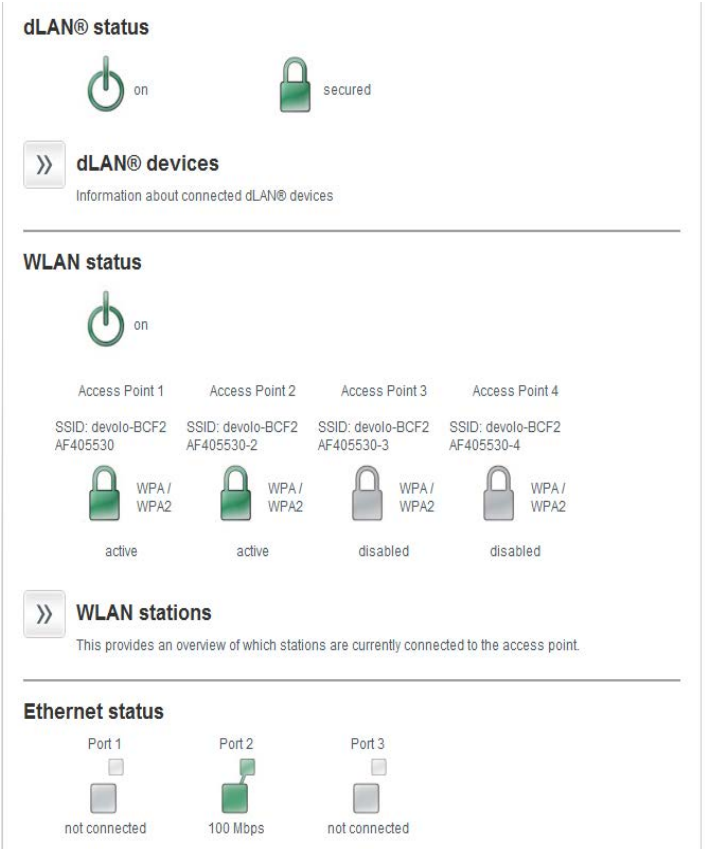


The five central areas of the configuration interface are displayed on the left edge. Click the button of an area to move directly into it.

- In the **Status overview** area, you get general information about all connected dLAN, WLAN and LAN devices.
- You can change or modify the various device settings for security, network, dLAN and time under **Device configuration**.
- You can change or modify WLAN settings in the **WLAN configuration** area.
- You can change or modify VLAN settings in the **VLAN configuration** area.
- The **Management** section is for resetting, securing and restoring your individual configurations. In addition, you can update the firmware of your dLAN 200 AVpro Wireless N here.

4.3 Status overview

In the **Status overview** area you can track the status of your connected dLAN, WLAN and LAN devices.


dLAN® status
on
secured
dLAN® devices
Information about connected dLAN® devices
WLAN status
on
Access Point 1
Access Point 2
Access Point 3
Access Point 4
SSID: devolo-BCF2 AF405530
SSID: devolo-BCF2 AF405530-2
SSID: devolo-BCF2 AF405530-3
SSID: devolo-BCF2 AF405530-4
WPA / WPA2
WPA / WPA2
WPA / WPA2
WPA / WPA2
active
active
disabled
disabled
WLAN stations
This provides an overview of which stations are currently connected to the access point.
Ethernet status
Port 1
Port 2
Port 3
not connected
100 Mbps
not connected

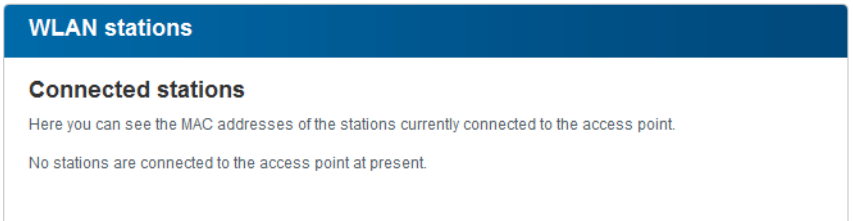
4.3.1 dLAN status

To display all connected dLAN devices, click either the **Ready to operate** icon or the **dLAN devices** arrow. Each connected dLAN device, regardless of whether it is connected locally or remote in the network, is displayed with its MAC address. Clicking the **lock** icon brings you directly to the **dLAN settings** (see **4.4.3 dLAN settings**).

dLAN® devices
dLAN® devices
List of all the dLAN® devices in the network.
dLAN 200 AVpro Wireless N (BC:F2:AF:40:48:0D) (Local device)

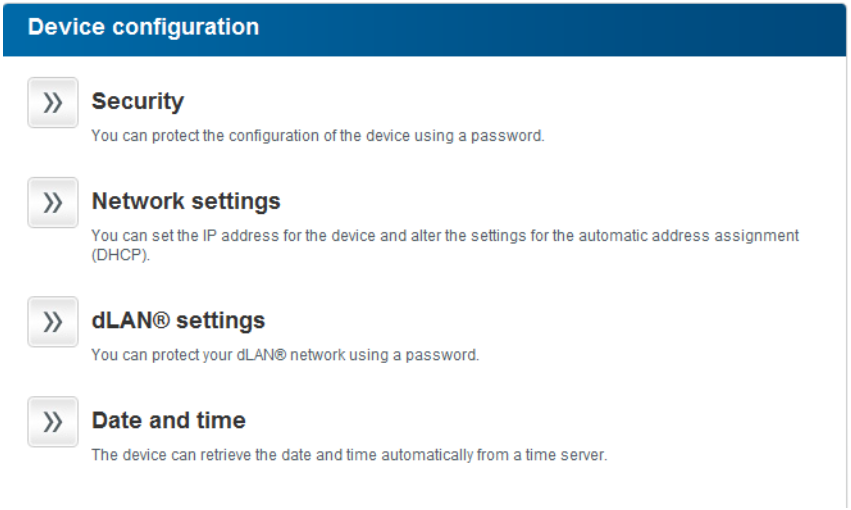
4.3.2 WLAN status

To display all connected WLAN devices, click either the **Ready to operate** icon or the **WLAN stations** arrow. Each connected WLAN client is displayed with its MAC address. Clicking the **lock** icon brings you directly to the **WLAN configuration** area (see **4.5 Disabling WLAN configuration**), where you can configure settings for WLAN network security.


WLAN stations
Connected stations
Here you can see the MAC addresses of the stations currently connected to the access point.
No stations are connected to the access point at present.

4.4 Device configuration

In the configuration area of the device you can modify settings for security, network, dLAN, date and time.


Device configuration
Security
You can protect the configuration of the device using a password.
Network settings
You can set the IP address for the device and alter the settings for the automatic address assignment (DHCP).
dLAN® settings
You can protect your dLAN® network using a password.
Date and time
The device can retrieve the date and time automatically from a time server.

4.4.1 Security

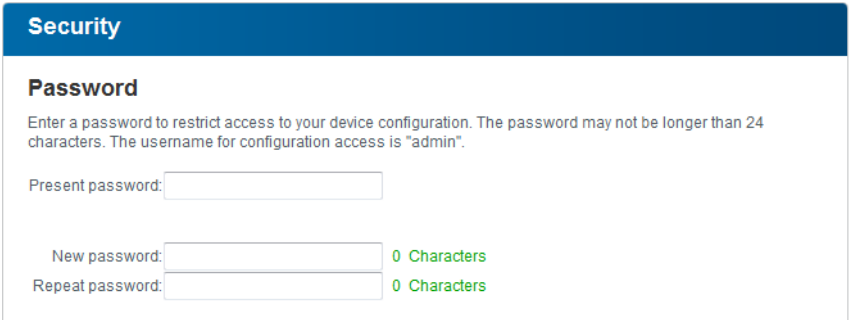
In this area you can control the access to the configuration interface as well as enable and disable the functions of the interfaces and buttons on the dLAN 200 AVpro Wireless N.

Password

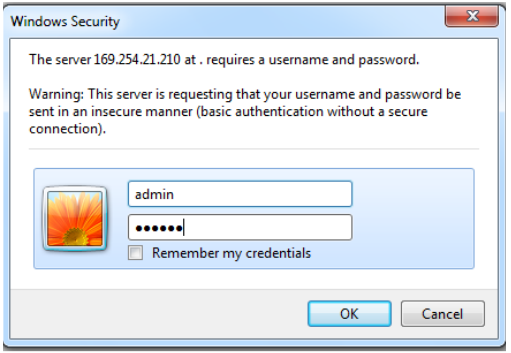
You can set a login password for access to the configuration interface.

By default, the built-in configuration interface of the dLAN 200 AVpro Wireless N is not protected with a password. However, we recommend assigning a password when the installation of the dLAN 200 AVpro Wireless N is complete to protect it against tampering by third parties.

① To do so, first enter (if present) the current password and then enter the desired new password twice. Now the configuration interface is protected against unauthorised access with your individual password!


Security
Password
Enter a password to restrict access to your device configuration. The password may not be longer than 24 characters. The username for configuration access is "admin".
Present password:
New password:
0 Characters
Repeat password:
0 Characters

② Call up the configuration interface again later; the following window appears first:


Windows Security
The server 169.254.21.210 at . requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
admin
Remember my credentials
OK
Cancel

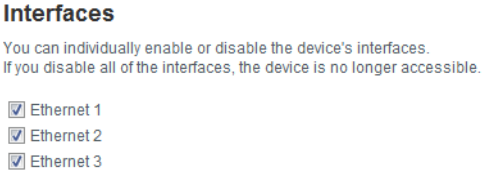
③ Enter **admin** in the **User name** field and your individual password in the **Password** field.

The* admin *user name cannot be changed.

Interfaces

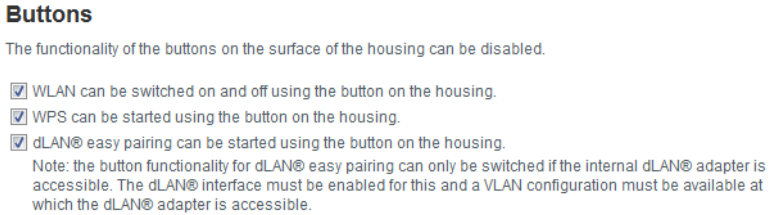
You can enable or disable the interface on the dLAN 200 AVpro Wireless N by enabling or disabling the corresponding options.

Note that the dLAN 200 AVpro Wireless N can no longer be reached once all interfaces have been switched off.


Interfaces
You can individually enable or disable the device's interfaces.
If you disable all of the interfaces, the device is no longer accessible.
Ethernet 1
Ethernet 2
Ethernet 3

Buttons

You can enable or disable the function of the **WLAN**, **WPS** and **dLAN encryption** buttons on the dLAN 200 AVpro Wireless N by enabling or disabling the corresponding options.


Buttons
The functionality of the buttons on the surface of the housing can be disabled.
WLAN can be switched on and off using the button on the housing.
WPS can be started using the button on the housing.
dLAN® easy pairing can be started using the button on the housing.
Note: the button functionality for dLAN® easy pairing can only be switched if the internal dLAN® adapter is accessible. The dLAN® interface must be enabled for this and a VLAN configuration must be available at which the dLAN® adapter is accessible.

Configuration over the web

The option **The device can be configured over the web** has to be enabled in order for the configuration interface to be accessible at all.

Disabling this option rules out the possibility of configuring and thus accessing the interface. This status can be reversed only by resetting the adapter to the factory defaults (see the* Reset *section).

Configuration over the web
Configuration over the web interface can be disabled
The device can be configured over the web

4.4.2 Network settings

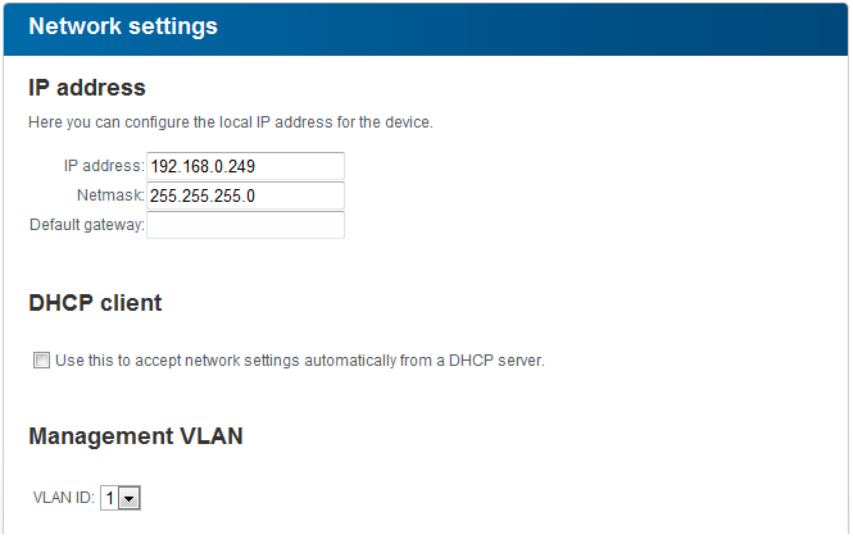
The dLAN 200 AVpro Wireless N also communicates via the TCP/IP protocol as a component of your home network. The IP address required for this can either be entered manually as a static address or obtained **automatically** from a **DHCP server**.

The option **Use this to accept network settings automatically from a DHCP server** is enabled in the factory defaults.

If a DHCP server is already present in the network for giving out IP addresses, have the option **Use this to accept network settings automatically from a DHCP server** enabled so that the dLAN 200 AVpro Wireless N automatically receives an address from it.

You can also assign a static IP address by making entries under **IP address** (e.g. '192.168.0.249') and **Netmask** (e.g. 255.255.255.0).

If you ever forget the IP address of your dLAN 200 AVpro Wireless N, open the **dLAN AVpro manager** *to find the device in the network. Proceed as described under* **4.1 Calling up the built-in configuration interface**.


Network settings
IP address
Here you can configure the local IP address for the device.
IP address: 192.168.0.249
Netmask: 255.255.255.0
Default gateway:
DHCP client
Use this to accept network settings automatically from a DHCP server.
Management VLAN
VLAN ID: 1

Management VLAN

If you use VLAN and have enabled it under **VLAN configuration**, specify a Management VLAN here by assigning the corresponding **VLAN ID** via the selection box.

The configuration interface can be accessed only via the management VLAN. The **factory defaults** of the dLAN 200 AVpro Wireless N have the **Management VLAN** configured with **VLAN ID 1**. Additionally, the DHCP server has to be accessible in the management VLAN, and thereby have the option **Use this to accept network settings automatically from a DHCP server** enabled.

If you ever "lock" yourself out of the interface, e.g. by deleting all VLANs, the adapter has to be returned to the factory defaults by being reset (see the* Reset *section).

If the management VLAN configuration is changed, please observe the sequence of the configuration steps to guarantee access to the configuration interface:

① Disable VLAN

② Configure VLAN port and PVID settings; save them

③ Under **Device configuration** ▷ **Network settings** ▷ **Management VLAN**, change the **VLAN ID** and save it

④ Re-enable VLAN

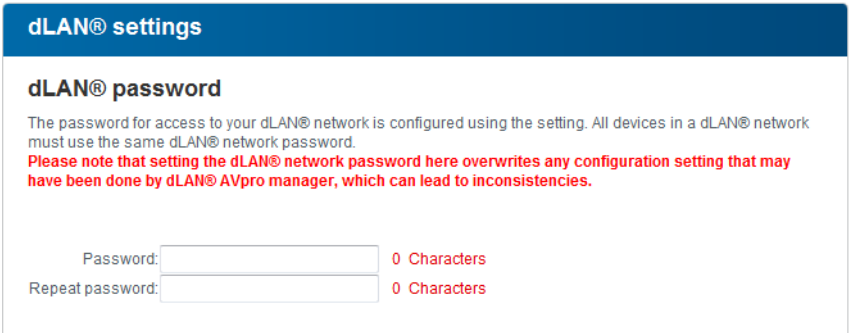
The settings for management VLAN are important only if the VLAN configuration is enabled.

4.4.3 dLAN settings

In a dLAN network, all connected components must use the same password. The dLAN password can be defined using **dLAN AVpro manager**, via the **dLAN encryption button** (see Chapter **5 dLAN network**) or in the **dLAN settings** section on the configuration interface.

When selecting the procedure, keep in mind the following:

- If the dLAN password is set using **dLAN AVpro manager** or via the **dLAN encryption button**, you can disregard the dLAN settings on the configuration interface, since the password is automatically forwarded.
- If the dLAN password is set or changed on the configuration interface, the password in **dLAN AVpro manager has to be adjusted** accordingly. The password is not forwarded automatically.

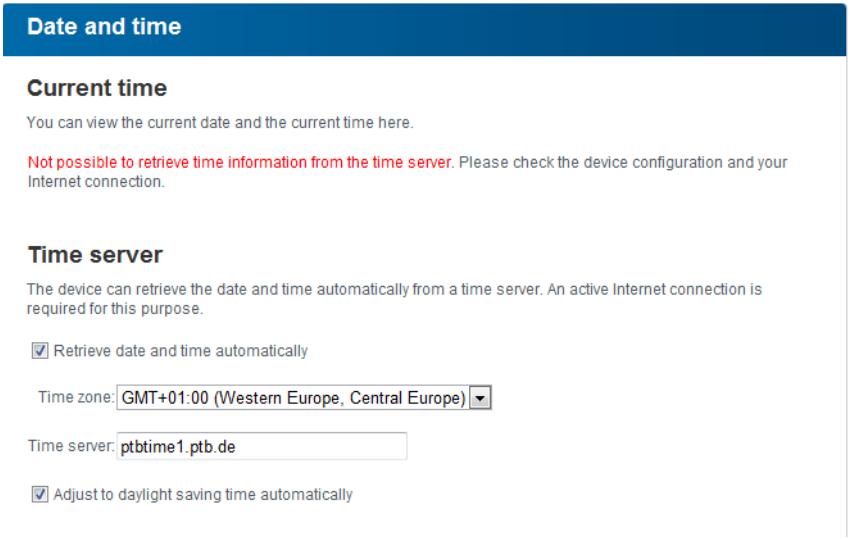

dLAN® settings
dLAN® password
The password for access to your dLAN® network is configured using the setting. All devices in a dLAN® network must use the same dLAN® network password.
Please note that setting the dLAN® network password here overwrites any configuration setting that may have been done by dLAN® AVpro manager, which can lead to inconsistencies.
Password:
0 Characters
Repeat password:
0 Characters

4.4.4 Time server

A time server is a server on the Internet whose task consists of providing the exact time. Most time servers are coupled with a radio clock.

To see which Internet time server your computer uses to communicate, simply click the clock in the lower right corner of the screen and select the **Internet time** *tab.*

Enable the option **Retrieve date and time automatically**, so that the dLAN 200 AVpro Wireless N can automatically synchronise the date and time. Select your **Time zone** and the **Time server**. If you have enabled the option **Adjust to daylight saving time automatically**, the dLAN 200 AVpro Wireless N automatically adjusts to daylight saving time.

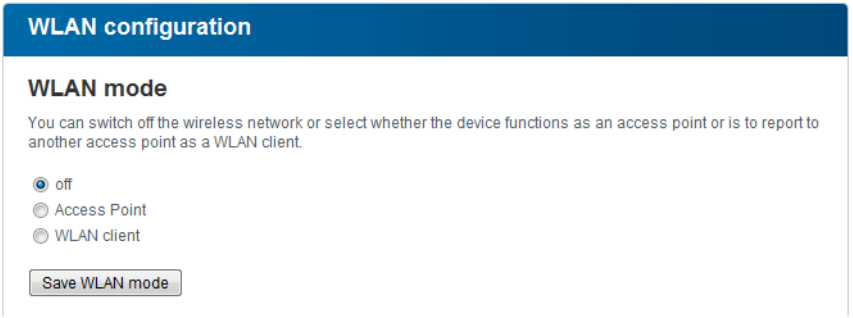

Date and time
Current time
You can view the current date and the current time here.
Not possible to retrieve time information from the time server. Please check the device configuration and your Internet connection.
Time server
The device can retrieve the date and time automatically from a time server. An active Internet connection is required for this purpose.
Retrieve date and time automatically
Time zone: GMT+01:00 (Western Europe, Central Europe)
Time server: ptbtime1.ptb.de
Adjust to daylight saving time automatically

4.5 Disabling WLAN configuration

If you would like, you can completely shut off the WLAN part of your dLAN 200 AVpro Wireless N, e.g. if you want to operate it exclusively as a simple dLAN device via the built-in Ethernet connections. To do so, under **WLAN configuration** select the **Off** mode and confirm your entry with **Save WLAN mode** or simply press the **WLAN ON/OFF** button on the housing.

Keep in mind that after saving this setting, you will be disconnected from any existing wireless connection to the dLAN 200 AVpro Wireless N. In this case, configure the device via Ethernet or dLAN.

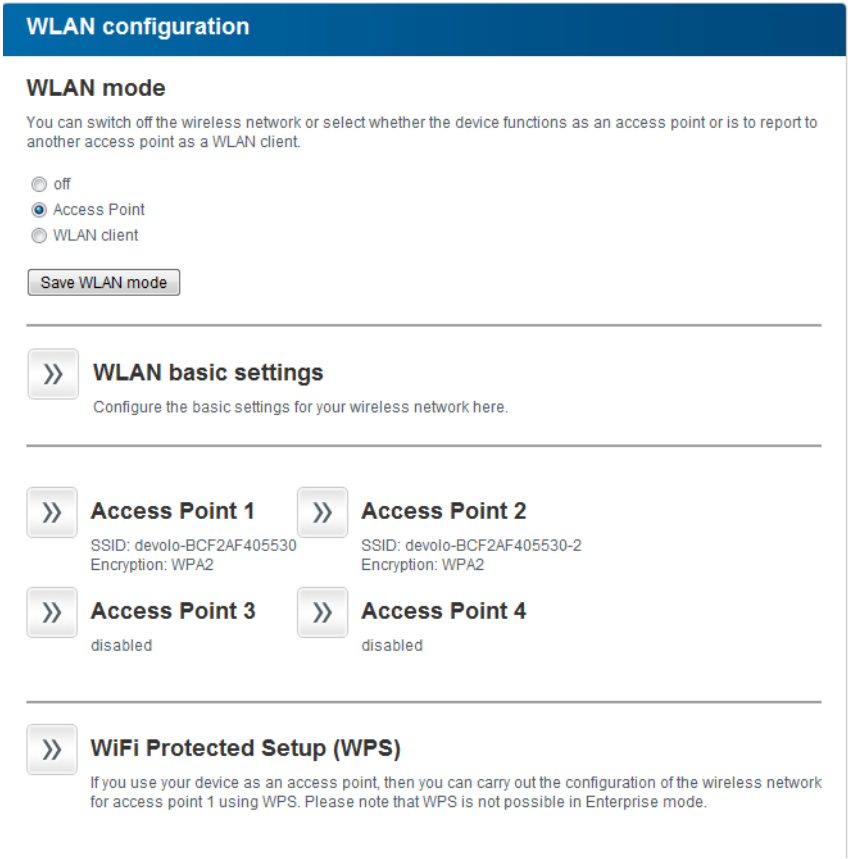
The operating state of the device is displayed under **4.3 Status overview**.


WLAN configuration
WLAN mode
You can switch off the wireless network or select whether the device functions as an access point or is to report to another access point as a WLAN client.
off
Access Point
WLAN client
Save WLAN mode

4.6 WLAN configuration as access point

If you would like the dLAN 200 AVpro Wireless N to act as an access point, select **Access point** mode under **WLAN configuration** and confirm your entry with **Save WLAN mode** or simply press the **WLAN ON/OFF** button on the housing. The dLAN 200 AVpro Wireless N automatically changes to Access point mode.

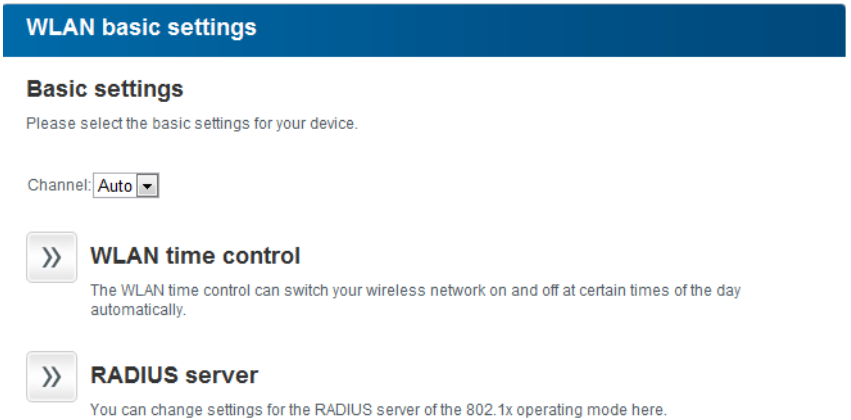
The operating state of the device is displayed under **4.3 Status overview**.


WLAN configuration
WLAN mode
You can switch off the wireless network or select whether the device functions as an access point or is to report to another access point as a WLAN client.
off
Access Point
WLAN client
Save WLAN mode
WLAN basic settings
Configure the basic settings for your wireless network here.
Access Point 1
SSID: devolo-BCF2AF405530
Encryption: WPA2
Access Point 2
SSID: devolo-BCF2AF405530-2
Encryption: WPA2
Access Point 3
disabled
Access Point 4
disabled
WiFi Protected Setup (WPS)
If you use your device as an access point, then you can carry out the configuration of the wireless network for access point 1 using WPS. Please note that WPS is not possible in Enterprise mode.

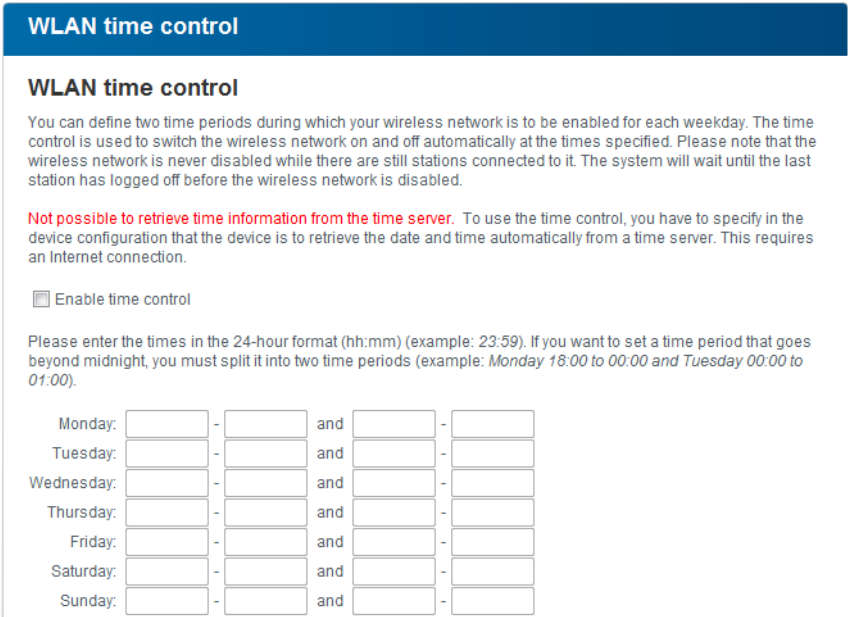
4.6.1 WLAN basic settings

In the WLAN basic settings you can set the time control and the RADIUS server, regardless of whether the dLAN 200 AVpro Wireless N acts as an access point or a client. These settings apply for both modes.

For operation as an access point, a (transmission) **channel** must be specified. There are 13 channels available. We recommend keeping the default setting **Auto**, since in this setting the dLAN 200 AVpro Wireless N selects the channel regularly and independently. In other words, if the last connected station logs out, a search for a suitable channel is carried out immediately. If no stations are connected, the device automatically selects a channel every 15 minutes.


WLAN basic settings
Basic settings
Please select the basic settings for your device.
Channel: Auto
WLAN time control
The WLAN time control can switch your wireless network on and off at certain times of the day automatically.
RADIUS server
You can change settings for the RADIUS server of the 802.1x operating mode here.

WLAN time control


WLAN time control
WLAN time control
You can define two time periods during which your wireless network is to be enabled for each weekday. The time control is used to switch the wireless network on and off automatically at the times specified. Please note that the wireless network is never disabled while there are still stations connected to it. The system will wait until the last station has logged off before the wireless network is disabled.
Not possible to retrieve time information from the time server. To use the time control, you have to specify in the device configuration that the device is to retrieve the date and time automatically from a time server. This requires an Internet connection.
Enable time control
Please enter the times in the 24-hour format (hh:mm) (example: 23:59). If you want to set a time period that goes beyond midnight, you must split it into two time periods (example: Monday 18:00 to 00:00 and Tuesday 00:00 to 01:00).
Monday:
Tuesday:
Wednesday:
Thursday:
Friday:
Saturday:
Sunday:
and

To be able to use the WLAN time control, the option **Retrieve date and time automatically** must ***be enabled*** under **Device configuration ⇨ Date and time**. ***An active Internet connection is also required. (see*** **4.4.4 Time server*)***

To be able to use the WLAN time control, enable the option **Enable time control**. The time control automatically switches your wireless network on and off at certain times of the day.

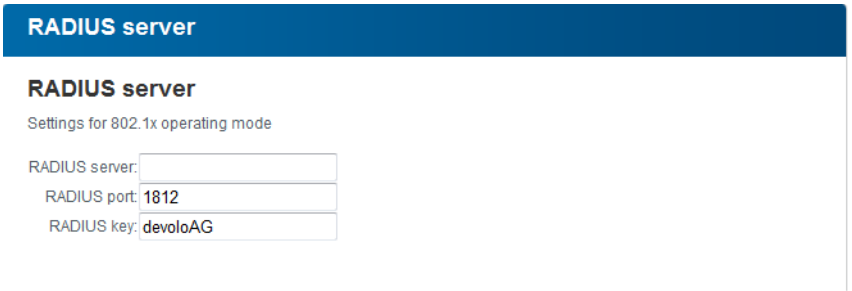
You can define two time periods during which your wireless network is to be enabled for each weekday. Then the time control automatically switches the wireless network on or off.

Keep in mind that, as long as the dLAN 200 AVpro Wireless N registers connected stations, the wireless network remains enabled. The wireless network is not switched off until the last station has logged off.

RADIUS server

In addition to the **WPA/WPA2** encryption key, the dLAN 200 AVpro Wireless N also supports **Enterprise Mode (see 4.6.2 Security settings for the access point** or **4.7.1 Security settings for the WLAN client**). In addition to the **client** and the **access point**, there is also the **RADIUS server** in Enterprise Mode. As a central authentication server, it assumes the user administration for multiple access points.

If you would like to use a **RADIUS server**, assign a name, **Radius port** and **Radius key**.



4.6.2 Security settings for the access point

If you want to enable this WLAN network, select **Enable this access point**.

The dLAN 200 AVpro Wireless N supports up to **4 SSIDs** or access points (**Multi SSID**), i.e. up to **4 WLAN networks** can be operated via the dLAN 200 AVpro Wireless N. The **SSID** specifies the name of your wireless network. You can see this name when logging onto the WLAN and thereby identify the correct subnet. If you enable the **Hide SSID** option, your wireless network remains hidden. In this case, potential network users must know the exact SSID and enter it manually to be able to set up a connection.

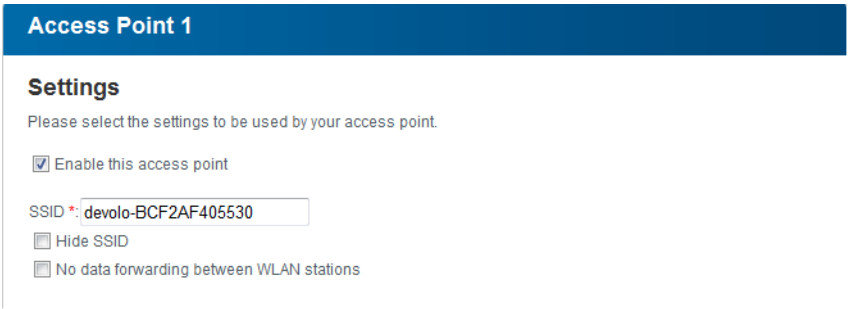
Changing the SSID setting can temporarily affect all existing connections.

Some WLAN clients have difficulty connecting to such hidden wireless networks. If the connection to a hidden SSID poses problems, first try to set up the connection with a visible SSID and only then try to hide it.

Depending upon the application scenario, security considerations may mean that it is to be forbidden for all devices to exchange data freely with each other. For this purpose, the option **No data forwarding between WLAN stations** can be enabled, which implements a genuine "peer-to-peer isolation"; all WLAN devices configured as client are not able to exchange any data with each other, but only with the dLAN 200 AVpro Wireless N.

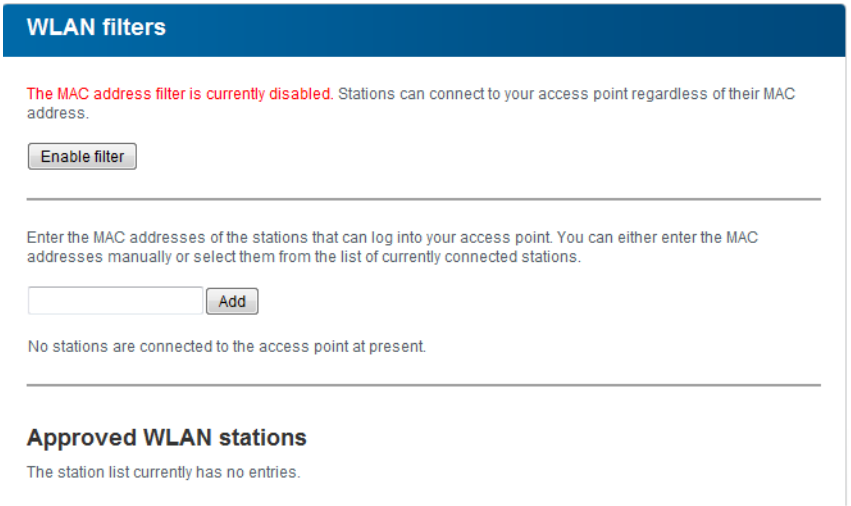
The factory defaults have this option disabled, i.e. all WLAN devices present in the network can freely exchange data with each other ("peer-to-peer" mode).

Only access point 1 supports the WPS function (see* 4.6.3 Wi-Fi Protected Setup (WPS)*).


Access Point 1
Settings
Please select the settings to be used by your access point.
Enable this access point
SSID *: devolo-BCF2AF405530
Hide SSID
No data forwarding between WLAN stations

WLAN filter

In addition to encryption, you can secure your wireless network even more by using a WLAN filter to limit access via WLAN to the dLAN 200 AVpro Wireless N for selected devices. Even if the encryption is switched off, the device will not establish a connection.


WLAN filters
The MAC address filter is currently disabled. Stations can connect to your access point regardless of their MAC address.
Enable filter
Enter the MAC addresses of the stations that can log into your access point. You can either enter the MAC addresses manually or select them from the list of currently connected stations.
Add
No stations are connected to the access point at present.
Approved WLAN stations
The station list currently has no entries.

The WLAN filter should be used only as an additional option. By using it you could limit access to your wireless network, but without encryption it would be relatively easy for third parties to eavesdrop on all of your data transmissions.

To use the WLAN filter, enable the option **Enable filters**. Now you can enter various network devices by means of what is known as your MAC address for access to your dLAN 200 AVpro Wireless N. Confirm each entry with **Add**. Network devices or stations connected to your dLAN 200 AVpro Wireless N are automatically listed, that is, to enable an already connected station for the dLAN 200 AVpro Wireless N, simply select the MAC address of the respective device and confirm it with **Add**. This then appears under **Approved WLAN stations**. To remove an enabled station, select its MAC address and confirm it with **Delete**.

The MAC address designates the hardware interface of each individual network device uniquely (e.g. the WLAN adapter of a computer or the Ethernet port of a printer). It consists of six double-digit hexadecimal numbers, each separated by a colon (e.g. 00:0B:3B:37:9D:C4). In general, the MAC address is on the housing of the device.

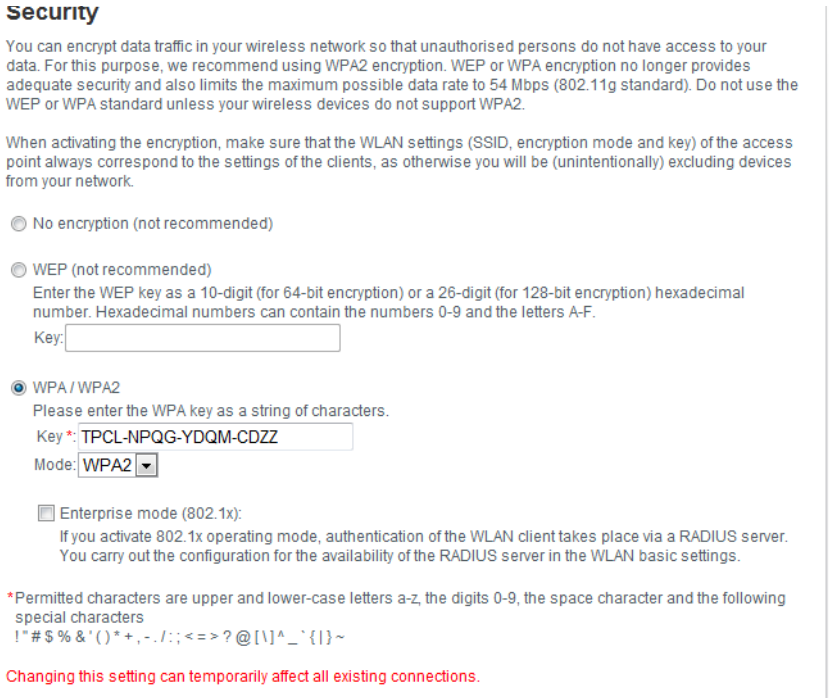
You can easily determine the MAC address of a Windows computer by opening the window with the command prompt under **Start** ⇨ **All Programs** ⇨ **Accessories** ⇨ **Command Prompt**. Enter the command **IPCONFIG /ALL** here. The MAC address is displayed under the designation **Physical address**.

After entering the MAC addresses, do not forget to click the **Save** button. If the entered values are incorrect (e.g. because the colons are missing), a corresponding error message is displayed.

Keep in mind that you also have to enter the MAC address of your own computer if you are connected to the dLAN 200 AVpro Wireless N not via the Ethernet port, but via WLAN. Otherwise you will block your own access to the device via WLAN by activating the WLAN filter!

Security (encryption)

Without encryption, not only are all data transmitted from client computers to the dLAN 200 AVpro Wireless N in your wireless network without protection, but there is also no password prompt to establish the connection. If no other security measures were set up, such as a WLAN filter (see Chapter **WLAN filter**), third parties can gain access to your network at any time and, for example, share your Internet connection. Usually this happens without you noticing it.


Security
You can encrypt data traffic in your wireless network so that unauthorised persons do not have access to your data. For this purpose, we recommend using WPA2 encryption. WEP or WPA encryption no longer provides adequate security and also limits the maximum possible data rate to 54 Mbps (802.11g standard). Do not use the WEP or WPA standard unless your wireless devices do not support WPA2.
When activating the encryption, make sure that the WLAN settings (SSID, encryption mode and key) of the access point always correspond to the settings of the clients, as otherwise you will be (unintentionally) excluding devices from your network.
No encryption (not recommended)
WEP (not recommended)
Enter the WEP key as a 10-digit (for 64-bit encryption) or a 26-digit (for 128-bit encryption) hexadecimal number. Hexadecimal numbers can contain the numbers 0-9 and the letters A-F.
Key:
WPA / WPA2
Please enter the WPA key as a string of characters.
Key *: TPCL-NPQG-YDQM-CDZZ
Mode: WPA2
Enterprise mode (802.1x):
If you activate 802.1x operating mode, authentication of the WLAN client takes place via a RADIUS server. You carry out the configuration for the availability of the RADIUS server in the WLAN basic settings.
*Permitted characters are upper and lower-case letters a-z, the digits 0-9, the space character and the following special characters
! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~
Changing this setting can temporarily affect all existing connections.

To secure the data transmission in your wireless network there are two security standards available.

- The older and weaker **WEP** standard can protect communication with the help of a key having either **10 or 26 hexadecimal characters**.
- The state-of-the-art **WPA and WPA2 (Wi-Fi Protected Access)** methods allow individualised keys consisting of **letters and numbers with a length of up to 63 characters**. You can simply enter them via the keyboard. Under **Mode**, you

can limit access of clients to the dLAN 200 AVpro Wireless N to the method you have selected. In addition to the **WPA/WPA2** encryption key, the dLAN 200 AVpro Wireless N also supports **Enterprise Mode**. As a central authentication server, the RADIUS server assumes the user administration (for multiple access points; **see RADIUS server**).

Enterprise Mode does* not *support any WPS.

Save all modified settings before leaving this configuration area again.

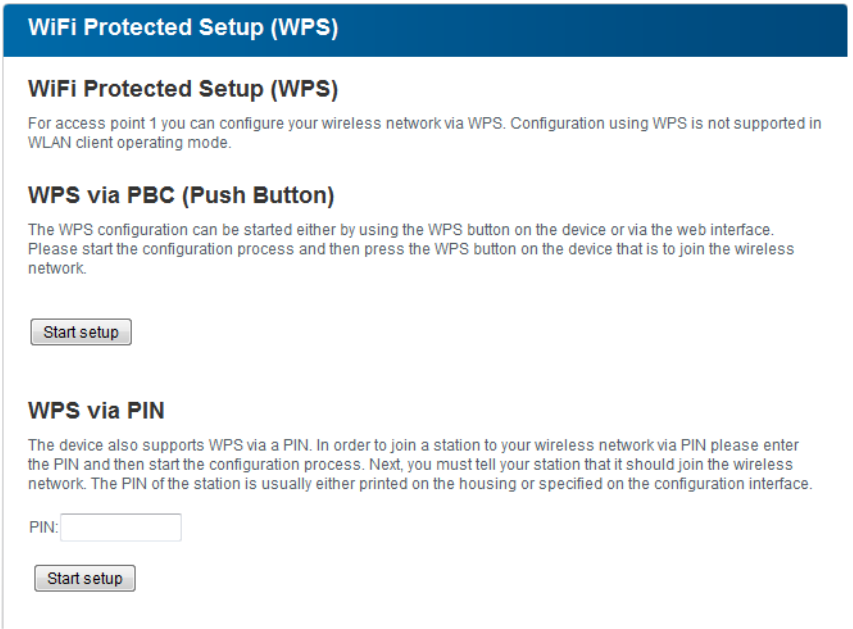
The* factory defaults *have the dLAN 200 AVpro Wireless N configured as an access point and the* WPA2 *WLAN encryption is set with the* security ID as the default WLAN key*. You will find the 16-character security ID on the label on the back of the housing.

When activating the encryption, make sure that the WLAN settings (SSID, encryption mode and encryption key) of the access point always correspond to the settings of the clients, as otherwise you will be (unintentionally) excluding devices from your network.

You should always encrypt the connections in your WLAN. Otherwise anyone within range could penetrate into your home network and, for example, share your Internet connection. Always select the better WPA2 encryption method if possible. Use WEP only if one of your wireless terminal devices does not operate with a better standard.

4.6.3 Wi-Fi Protected Setup (WPS)

Wi-Fi Protected Setup (WPS) is one of the international encryption standards developed by the Wi-Fi Alliance for easily and quickly setting up a secure wireless network. The encryption keys of the respective WLAN client are transmitted automatically and continuously to the other WLAN client(s) of the wireless network. The dLAN 200 AVpro Wireless N offers two different variants for transmitting these encryption keys:


WiFi Protected Setup (WPS)
WiFi Protected Setup (WPS)
For access point 1 you can configure your wireless network via WPS. Configuration using WPS is not supported in WLAN client operating mode.
WPS via PBC (Push Button)
The WPS configuration can be started either by using the WPS button on the device or via the web interface. Please start the configuration process and then press the WPS button on the device that is to join the wireless network.
Start setup
WPS via PIN
The device also supports WPS via a PIN. In order to join a station to your wireless network via PIN please enter the PIN and then start the configuration process. Next, you must tell your station that it should join the wireless network. The PIN of the station is usually either printed on the housing or specified on the configuration interface.
PIN:
Start setup

WPS via PBC (Push Button Configuration):

① Start the encryption process on the dLAN 200 AVpro Wireless N

- ○ either by pressing the **WPS button** on the **front panel of the device** or
- ○ by pressing the **Start setup** button on the user interface under **WLAN configuration** ▷ **Wi-Fi Protected Setup (WPS)**.

② Then press either the WPS key of the WLAN client you are adding or the WPS button on the configuration interface. Now the devices exchange their

encryption keys and establish a secure WLAN connection. The WLAN LED on the front panel indicates the synchronisation process by flashing.

WPS via PIN:

① To interconnect WLAN clients securely in your wireless network via PIN variants, enter an individualised key in the configuration interface under **WLAN configuration ⇨ Wi-Fi Protected Setup (WPS) ⇨ PIN** and start the encryption process by pressing the **Start setup** button.

② Open the configuration interface of the WLAN client to be added and transmit the PIN selected on the dLAN 200 AVpro Wireless N. Confirm the encryption process as described there. Now the devices exchange their encryption keys and establish a secure WLAN connection. The WLAN LED on the front panel indicates the synchronisation process by flashing.

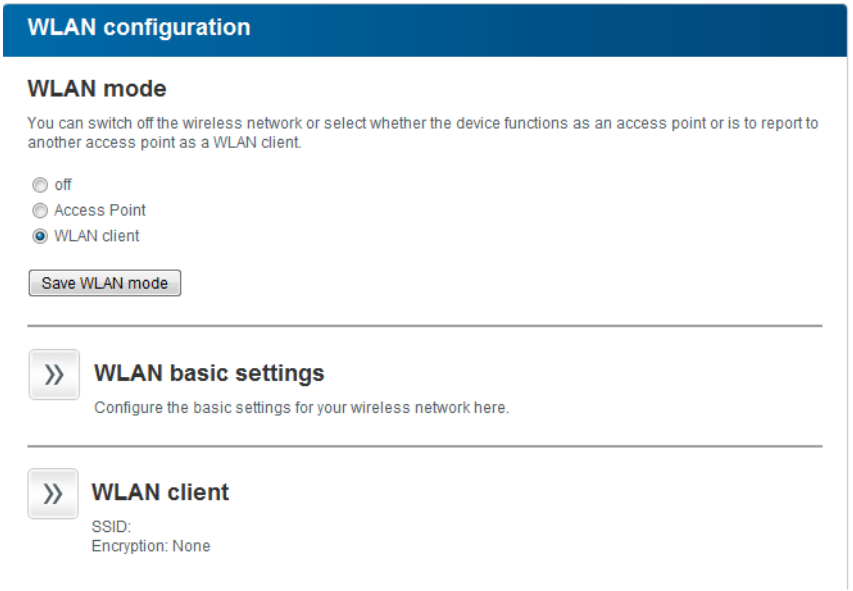
Use of the **WPS** process implies either **WPA** or **WPA2**. For that reason, keep in mind the following automatic settings depending on the encryption standard (also refer to **4.4.1 Security**), i.e.

- if under **WLAN configuration ⇨ Access Point No encryption** or **WEP** is selected in advance, **WPA2** is set automatically. The newly generated password is displayed under **WLAN configuration ⇨ Access Point** in the **Key** field.
- if under **WLAN configuration ⇨ Access Point WEP** is selected in advance, **WPA2** is set automatically. The newly generated password is displayed under **WLAN configuration ⇨ Access Point** in the **Key** field.
- if under **WLAN configuration ⇨ Access Point WPA** is selected in advance, this setting remains with the previously assigned password.
- if under **WLAN configuration ⇨ Access Point WPA2** is selected in advance, this setting remains with the previously assigned password.

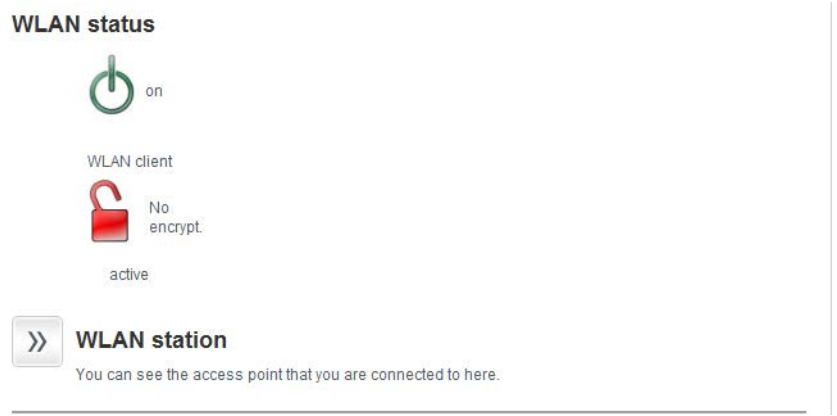
The WPS function is supported only by access point 1.

4.7 WLAN configuration as client

If you would like the dLAN 200 AVpro Wireless N to act as client, select **WLAN client** mode under **WLAN configuration** and confirm your entry with **Save WLAN mode**.


WLAN configuration
WLAN mode
You can switch off the wireless network or select whether the device functions as an access point or is to report to another access point as a WLAN client.
off
Access Point
WLAN client
Save WLAN mode
WLAN basic settings
Configure the basic settings for your wireless network here.
WLAN client
SSID:
Encryption: None

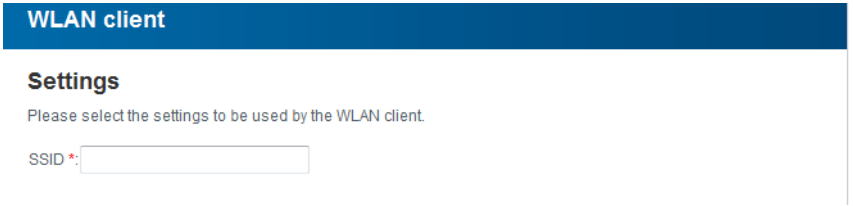
The operating state of the device is displayed under **Status display**.



You can find a detailed description of the WLAN basic settings under **4.6.1 WLAN basic settings**.

4.7.1 Security settings for the WLAN client

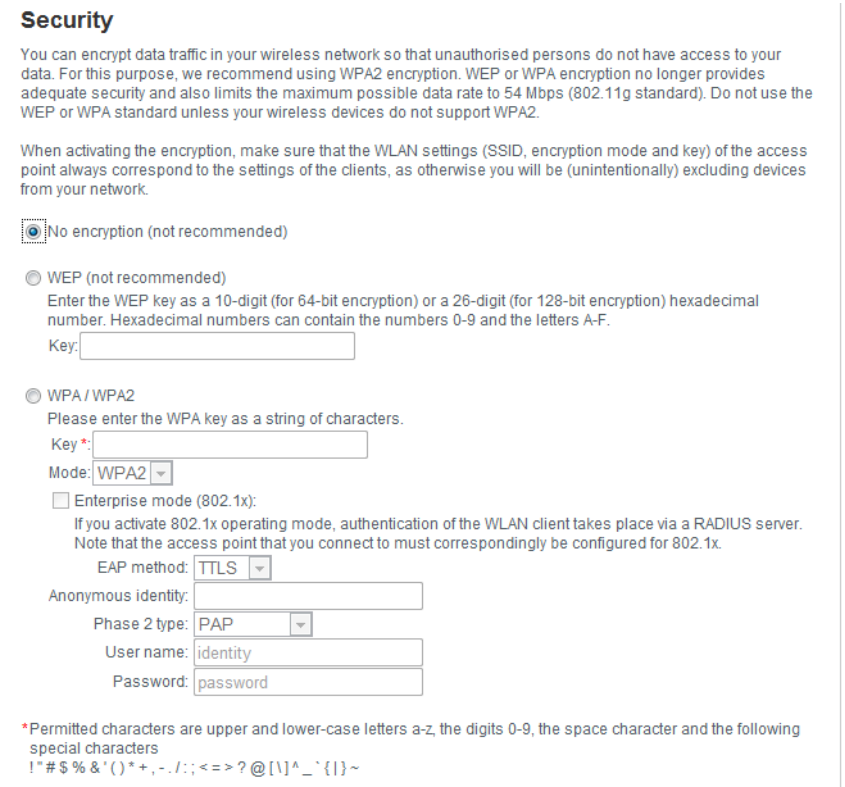
In the **SSID** field, enter the SSID of the corresponding access point.



To secure the data transmission in your wireless network there are two security standards available.

- The older and weaker **WEP** standard can protect communication with the help of a key having either **10 or 26 hexadecimal characters**.
- The state-of-the-art **WPA and WPA2 (Wi-Fi Protected Access)** methods allow individualised keys consisting of **letters and numbers with a length of up to 63 characters**. You can simply enter them via the keyboard. Under **Mode**, you can limit access of clients to the dLAN 200 AVpro Wireless N to the method you have selected. In addition to the **WPA/WPA2** encryption key, the dLAN 200 AVpro Wireless N also supports **Enterprise Mode.** As a central authentication server, the RADIUS server assumes the user administration (for multiple access points; **see RADIUS server**).

Enterprise Mode does* not *support any WPS.


Security
You can encrypt data traffic in your wireless network so that unauthorised persons do not have access to your data. For this purpose, we recommend using WPA2 encryption. WEP or WPA encryption no longer provides adequate security and also limits the maximum possible data rate to 54 Mbps (802.11g standard). Do not use the WEP or WPA standard unless your wireless devices do not support WPA2.
When activating the encryption, make sure that the WLAN settings (SSID, encryption mode and key) of the access point always correspond to the settings of the clients, as otherwise you will be (unintentionally) excluding devices from your network.
No encryption (not recommended)
WEP (not recommended)
Enter the WEP key as a 10-digit (for 64-bit encryption) or a 26-digit (for 128-bit encryption) hexadecimal number. Hexadecimal numbers can contain the numbers 0-9 and the letters A-F.
Key:
WPA / WPA2
Please enter the WPA key as a string of characters.
Key *:
Mode: WPA2
Enterprise mode (802.1x):
If you activate 802.1x operating mode, authentication of the WLAN client takes place via a RADIUS server. Note that the access point that you connect to must correspondingly be configured for 802.1x.
EAP method: TTLS
Anonymous identity:
Phase 2 type: PAP
User name: identity
Password: password
*Permitted characters are upper and lower-case letters a-z, the digits 0-9, the space character and the following special characters
! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

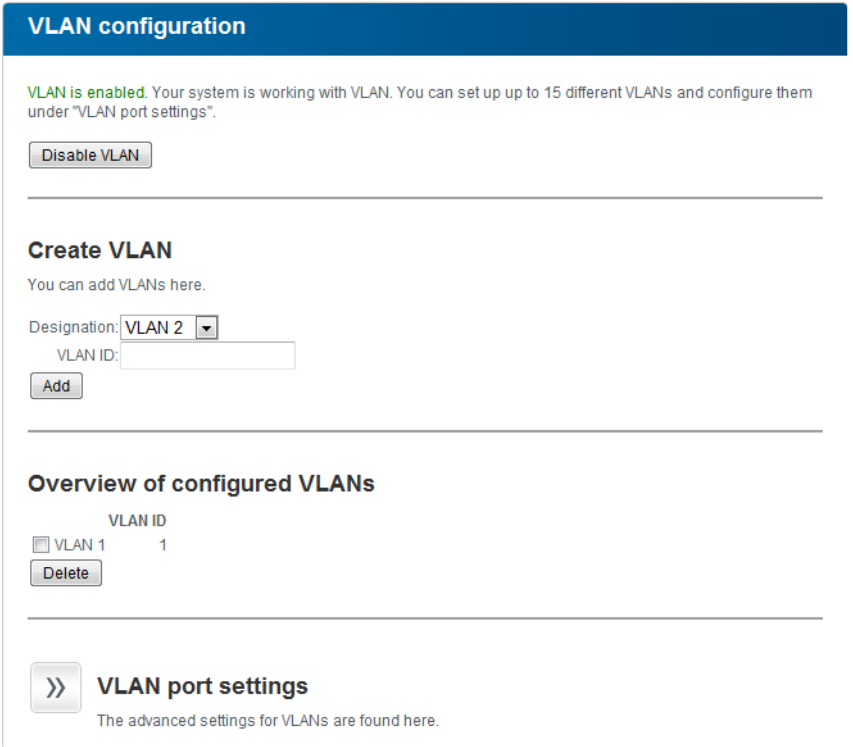
Save all modified settings before leaving this configuration area again.

The* factory defaults *have the dLAN 200 AVpro Wireless N configured as an access point and the* WPA2 *WLAN encryption is set with the* security ID as the default WLAN key*. You will find the 16-character security ID on the label on the back of the housing.

When activating the encryption, make sure that the WLAN settings (SSID, encryption mode and encryption key) of the access point always correspond to the settings of the clients, as otherwise you will be (unintentionally) excluding devices from your network.

4.8 VLAN configuration

You can select whether you would like to disable the VLAN configuration completely or use it. To do so, press the **Enable VLAN** or **Disable VLAN** button. If VLAN is disabled, all Ethernet ports, the dLAN port and the WLAN access points are interconnected, i.e. in this operating mode the VLAN settings have no influence on the behaviour of the dLAN 200 AVpro Wireless N.


VLAN configuration
VLAN is enabled. Your system is working with VLAN. You can set up up to 15 different VLANs and configure them under "VLAN port settings".
Disable VLAN
Create VLAN
You can add VLANs here.
Designation: VLAN 2
VLAN ID:
Add
Overview of configured VLANs
VLAN ID
VLAN 1 1
Delete
VLAN port settings
The advanced settings for VLANs are found here.

4.8.1 Create VLAN

The factory defaults have VLAN 1 configured with VLAN ID 1. You can configure additional VLANs under **Create VLAN**. In doing so, a VLAN (VLAN 1 to VLAN 15) has to be selected and a VLAN ID (1 to 4094) assigned. When creating VLANs, already assigned VLAN IDs cannot be assigned a second time. Configured VLANs are illustrated in the overview.

When configuring the VLANs, the VLAN port settings and when defining the Management VLAN, the configuration interface of the dLAN 200 AVpro Wireless N should remain accessible, i.e. configurable. If you ever "lock" yourself out in spite of this, the adapter has to be returned to the factory defaults by being reset (see the* Reset *section).

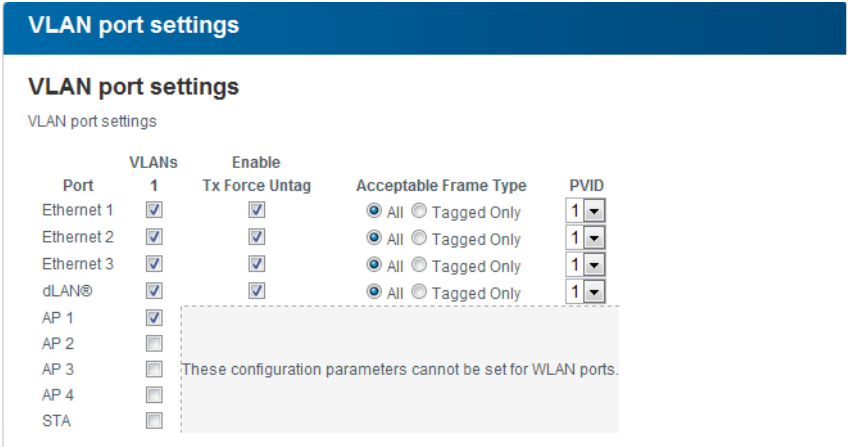
4.8.2 Overview of configured VLANs

To delete a VLAN, first enable it and then confirm with **Delete**. It is not possible to delete all VLANs; one VLAN must remain configured.

An enabled VLAN configuration requires at least one configured VLAN, since otherwise the configuration interface is no longer accessible and no connection of the port is enabled.

4.8.3 VLAN port settings

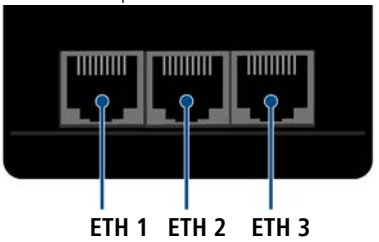
The VLAN port settings are configured here.



The existing ports of the dLAN 200 AVpro Wireless N are listed in the first left column.

The configured VLANs are listed in the row header.

The ports can be assigned to the VLANs via the matrix. Multiple VLANs can be assigned to the Ethernet ports and the dLAN port.



WLAN ports can be assigned only to a VLAN.

For more detailed help on verifying the settings, refer to our online FAQs on our website at www.devolo.com*.*

If the WLAN mode **Access Point** is enabled, only the access points are assigned to the VLANs. If the WLAN mode **WLAN client** is enabled, only the WLAN client is assigned to the VLAN.

The behaviour of the port is configured via the columns **Enable Tx Force Untag**, **Acceptable Frame Type (All/Tagged only)** and **PVID**:

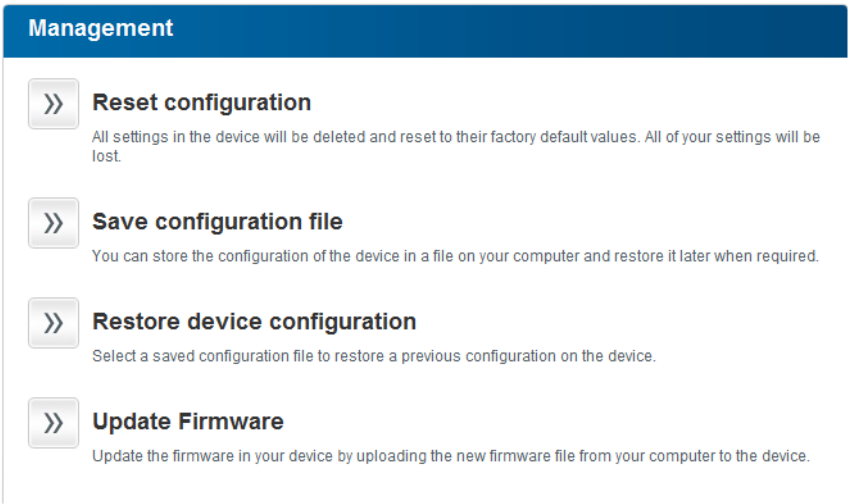
- If the option **Enable Tx Force Untag** is enabled, all **outgoing frames** are sent from this port as **"untagged"**.
- If **Enable Tx Force Untag** is **not** enabled, all **outgoing frames** are sent from this port as "**tagged"**.

The **factory defaults** *of the dLAN 200 AVpro Wireless N have the option* **Enable Tx Force Untag enabled***, i.e. all frames are sent "untagged".*

- The option **Acceptable Frame Type (All/Tagged only)** refers to the incoming data path of the ports. It determines whether all frames i.e. "tagged" and "untagged" (**All**) are accepted or only "tagged" frames (**Tagged Only**). If the **All** setting is enabled, all "untagged" frames are forwarded to the VLAN with the PVID configured for this port.
- Under **PVID** the **VLAN ID** is specified, which is assigned **received** "**untagged"** frames. In the setting **Acceptable Frame Type (Tagged only)** the configured PVID is insignificant.

4.9 Management

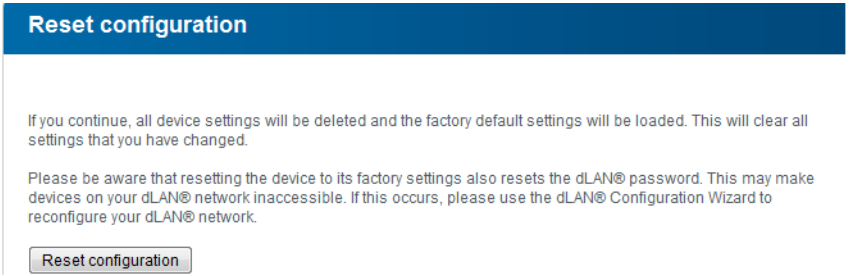
In the **Management** area you can reset the current configuration to the factory defaults, save it to your computer as a file or restore it from there and update the firmware of the dLAN 200 AVpro Wireless N.


Management
Reset configuration
All settings in the device will be deleted and reset to their factory default values. All of your settings will be lost.
Save configuration file
You can store the configuration of the device in a file on your computer and restore it later when required.
Restore device configuration
Select a saved configuration file to restore a previous configuration on the device.
Update Firmware
Update the firmware in your device by uploading the new firmware file from your computer to the device.

4.9.1 Resetting the configuration

With the **Management** ⇨ **Reset configuration** command, the dLAN 200 AVpro Wireless N is reset to the original factory defaults. In doing so, you lose your personal settings.

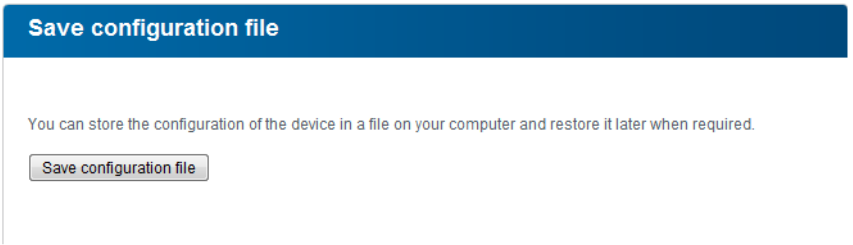
The last-assigned dLAN password for the dLAN 200 AVpro Wireless N is also reset. To re-secure your dLAN AVpro network individually, read further at **4.4.3 dLAN settings**.


Reset configuration
If you continue, all device settings will be deleted and the factory default settings will be loaded. This will clear all settings that you have changed.
Please be aware that resetting the device to its factory settings also resets the dLAN® password. This may make devices on your dLAN® network inaccessible. If this occurs, please use the dLAN® Configuration Wizard to reconfigure your dLAN® network.
Reset configuration

For backup purposes, all active configuration settings can be transmitted to your computer, stored there as a file and reloaded into the dLAN 200 AVpro Wireless N. In this way, you can for example generate configurations for different network environments, with which you can set up the device quickly and easily.

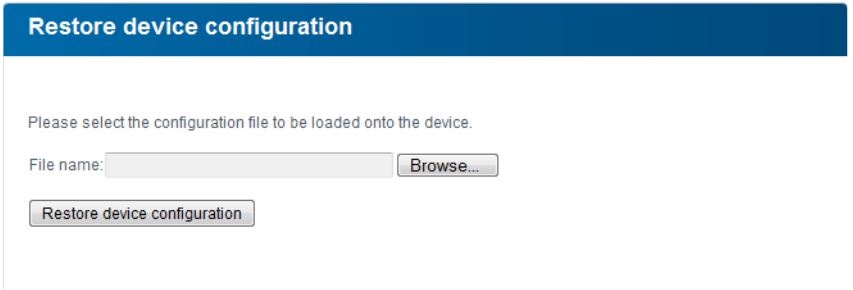
4.9.2 Saving a configuration file

To save the active configuration to your computer as a file, select the corresponding button in the area **Management** ⇨ **Save configuration file**. Then enter a storage location and name for the settings file.


Save configuration file
You can store the configuration of the device in a file on your computer and restore it later when required.
Save configuration file

4.9.3 Restoring a configuration

An existing configuration file can be sent to the dLAN 200 AVpro Wireless N in the area **Management ⇨ Restore device configuration** and enabled there. Select a suitable file via the **Browse…** button and start the operation by clicking the **Restore device configuration** button.


Restore device configuration
Please select the configuration file to be loaded onto the device.
File name:
Browse...
Restore device configuration

4.9.4 Update firmware

The firmware of the dLAN 200 AVpro Wireless N includes the software for operating the device. If necessary, devolo offers new versions on the Internet as a file download, for example to modify existing functions.

① To bring the firmware up to the latest version, first go to the devolo website, www.devolo.com, and download the appropriate file for the dLAN 200 AVpro Wireless N to your computer.

② Then in the configuration dialogue, go to the area **Management** ▷ **Update Firmware**. Click **Browse…** and select the downloaded file.

③ Then start the update procedure with the **Update Firmware** button. After a successful update, the dLAN 200 AVpro Wireless N restarts automatically.

Ensure that the update procedure is not interrupted. To do so, it is best to connect your computer to the dLAN 200 AVpro Wireless N via dLAN or LAN rather than WLAN.

5 dLAN network

5.1 Security in the dLAN

Before you can use the dLAN 200 AVpro Wireless N in your dLAN network, first you have to connect it to other dLAN AVpro devices as a home network. Two specific pieces of information are especially important for this:

- Shared use of the dLAN password serves as access control to the dLAN network and results in a delimited dLAN network.
- Shared use of a dLAN password serves as encryption of the dLAN network, and thereby the interception protection, of the transmitted data.

The dLAN password can be specified automatically via the encryption button or manually using the dLAN AVpro manager program. Please note the following basic principle when choosing your encryption method:

- In dLAN AVpro networks, data encryption is as simple as touching a button, since all corresponding dLAN AVpro devices are equipped with an encryption button.
- For dLAN AVpro networks that include devices with and without encryption buttons, data encryption must be set up using the dLAN AVpro manager.

5.2 dLAN AVpro network encryption at the touch of a button

To encrypt a dLAN AVpro network, in which all associated devices are equipped with an encryption button, simply press the encryption button that is located on the device. Pressing this button will encrypt your dLAN AVpro network with a randomly generated password.

For security reasons, the function of the encryption button can be disabled in the dLAN AVpro manager or on the configuration interface under 4.4 Device configuration***.***

The following section contains exact instructions of encryption on the basis of possible network scenarios:

Adapters cannot be configured while in Standby mode.

Encrypting a new dLAN AVpro network with a dLAN 200 AVpro Wireless N and an additional dLAN AVpro adapter (Fig. 4)

Once both dLAN AVpro adapters have been successfully connected, press each encryption button for >one second within two minutes of one another.

That's it! Your dLAN AVpro network is now protected against unauthorised access.

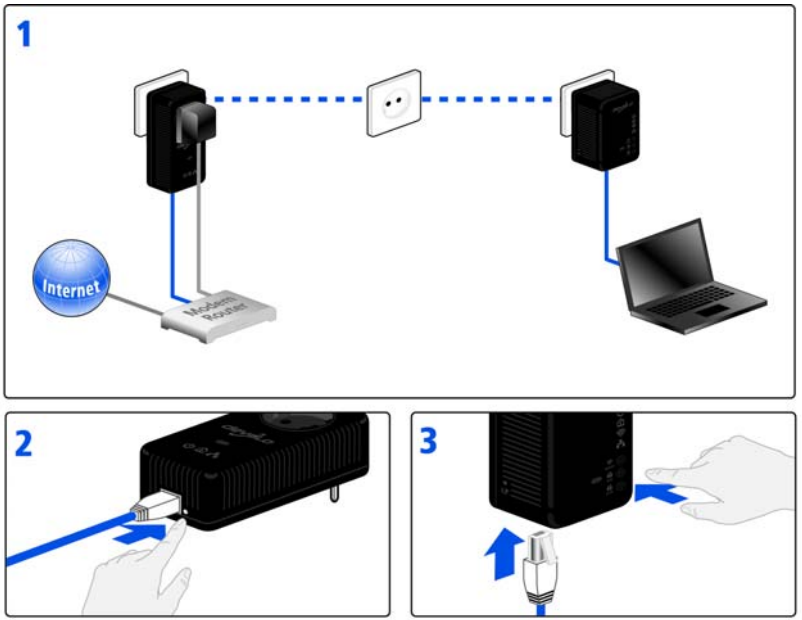


Fig. 4

Expanding an existing dLAN AVpro network by adding another dLAN AVpro adapter (Fig. 5)

If you have already secured your existing dLAN AVpro network using the encryption button, use the same method to integrate further adapters. Once you have successfully connected the new dLAN AVpro adapter, first press the encryption button (> one second) of one of your network's existing adapters, then press the encryption button (> one second) of your new dLAN AVpro adapter within two minutes.

That's it! The new dLAN AVpro adapter is now integrated in your network. To integrate additional dLAN AVpro adapters in your network, repeat the above steps.

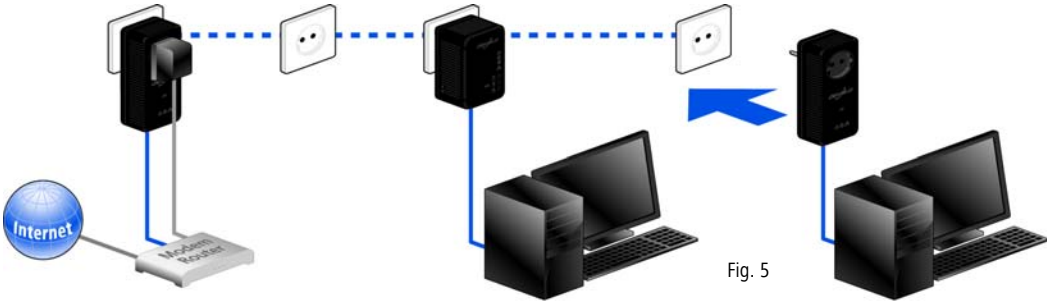


Fig. 5

Removing a dLAN AVpro adapter from a network (Fig. 6)

To remove a dLAN 200 AVpro Wireless N or another dLAN AVpro adapter from an existing network, press its encryption button for at least ten seconds. The device will be assigned a new randomly generated password and will thus no longer be able to access the network. To integrate the device into a different dLAN AVpro network, follow the steps described above, depending on whether you are setting up a new network or adding the adapter to an existing one.

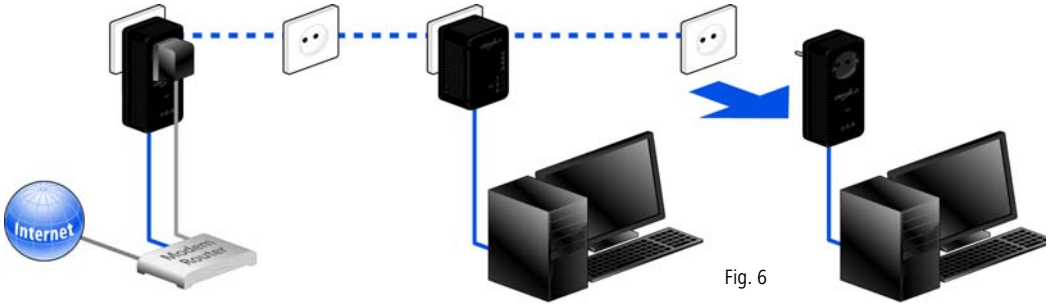


Fig. 6

5.3 dLAN AVpro manager for Windows

The installation wizard installs the devolo dLAN AVpro manager configuration software as well as the associated manual on the Windows operating system (see 3.4.1 Software for Windows).

In addition to the individual encryption of your dLAN network and the security from unauthorised access, **devolo dLAN AVpro manager** offers other expanded dLAN functions.

For detailed descriptions and information on configuration of your dLAN network please consult this devolo dLAN AVpro manager manual.

6 Appendix

For the permitted voltage range for operating the device and the power consumption, refer to the label on the rear side of the device. Additional technical information is available on the product sheet.

6.1 Important safety instructions

All safety and operating instructions should be read and understood before using the device, and should be kept for future reference.

- Never open the device. There are no user-serviceable parts inside the device.

Do not try to service this product yourself! Contact qualified technicians each and every time your device needs maintenance. There is a risk of electric shock!

- Use the device in a dry location only.

The outlet must be within reach of the connected network device. The dLAN 200 AVpro Wireless N and the network device must be easily accessible.

- To switch the device off, pull the power plug out of the power outlet.
- To disconnect the device from the power supply grid, pull the power plug.
- Do not keep the device in direct sunlight.
- Do not insert any objects into the openings of the device.
- Slots and openings on the case serve as ventilation. Never block or cover them.
- Never set up the device near a heater or radiator.
- The device should be located only where sufficient ventilation can be ensured.
- Disconnect the device from the power supply grid before cleaning. Use a moist towel to clean the device. Never use water, paint thinner, benzene, alcohol or other strong cleaning agents when cleaning the device, as these could damage the case.
- Never use the device with a power supply that does not meet the specifications provided on the rating plate.
- In the event of damage, disconnect the device from the power supply grid and contact customer service. This applies, for example, if

- the power cable or plug is damaged.
- liquid has been spilled on the device or objects have fallen into the device.
- the device has been exposed to rain or water.
- the device does not work, even though the operating instructions have been followed properly.
- the device's case is damaged.

6.2 Disposal of old devices

To be used in the countries of the European Union and other European countries with a separate collecting system:

The icon with crossed-out wastebasket on the device means that this adapter is an electrical or electronic device that falls within the scope of application of the German Electrical and Electronic Equipment Act ("Elektrogesetz"). Since 24 March 2006, these types of devices may no longer be disposed of with household waste. Rather, in Germany, they can be given to a municipal collection point free of charge. Contact your municipal government to find out the address and hours of the nearest collection point.

6.3 Warranty conditions

The devolo AG warranty is given to purchasers of devolo products in addition to the warranty conditions provided by law and in accordance with the following conditions:

1 Warranty coverage

a) The warranty covers the equipment delivered and all its parts. Parts will, at devolo's sole discretion, be replaced or repaired free of charge if, despite proven proper handling and adherence to the operating instructions, these parts became defective due to fabrication and/or material defects. Alternatively, devolo reserves the right to replace the defective product with a comparable product with the same specifications and features. Operating manuals and possibly supplied software are excluded from the warranty.

b) Material and service charges shall be covered by devolo, but not shipping and handling costs involved in transport from the buyer to the service station and/or to devolo.

c) Replaced parts become property of devolo.

d) devolo is authorized to carry out technical changes (e.g. firmware updates) beyond repair and replacement of defective parts in order to bring the equipment up to the current technical state. This does not result in any additional charge for the customer. A legal claim to this service does not exist.

2 Warranty period

The warranty period for this devolo product is three years. This period begins at the day of delivery from the devolo dealer. Warranty services carried out by devolo do not result in an extension of the warranty period nor do they initiate a new warranty period. The warranty period for installed replacement parts ends with the warranty period of the device as a whole.

3 Warranty procedure

a) If defects appear during the warranty period, the warranty claims must be made immediately, at the latest within a period of 7 days.

b) In the case of any externally visible damage arising from transport (e.g. damage to the housing), the person carrying out the transportation and the sender should be informed immediately. On discovery of damage which is not externally visible, the transport company and the sender are to be immediately informed in writing, at the latest within 3 days of delivery.

c) Transport to and from the location where the warranty claim is accepted and/or the repaired device is exchanged, is at the purchaser's own risk and cost.

d) Warranty claims are only valid if a copy of the original purchase receipt is returned with the device. devolo reserves the right to require the submission of the original purchase receipt.

4 Suspension of the warranty

All warranty claims will be deemed invalid

a) if the label with the serial number has been removed from the device,

b) if the device is damaged or destroyed as a result of acts of nature or by environmental influences (moisture, electric shock, dust, etc.),

c) if the device was stored or operated under conditions not in compliance with the technical specifications,

d) if the damage occurred due to incorrect handling, especially to non-observance of the system description and the operating instructions,

e) if the device was opened, repaired or modified by persons not contracted by devolo,

f) if the device shows any kind of mechanical damage, or

g) if the warranty claim has not been reported in accordance with 3a) or 3b).

5 Operating mistakes

If it becomes apparent that the reported malfunction of the device has been caused by unsuitable hardware, software, installation or operation, devolo reserves the right to charge the purchaser for the resulting testing costs.

6 Additional regulations

The above conditions define the complete scope of devolo's legal liability.

a) The warranty gives no entitlement to additional claims, such as any refund in full or in part. Compensation claims, regardless of the legal basis, are excluded. This does not apply if e.g. injury to persons or damage to private property are specifically covered by the product liability law, or in cases of intentional act or culpable negligence.

b) Claims for compensation of lost profits, indirect or consequential detriments, are excluded.

c) devolo is not liable for lost data or retrieval of lost data in cases of slight and ordinary negligence.

d) In the case that the intentional or culpable negligence of devolo employees has caused a loss of data, devolo will be liable for those costs typical to the recovery of data where periodic security data back-ups have been made.

e) The warranty is valid only for the first purchaser and is not transferable.

f) The court of jurisdiction is located in Aachen, Germany in the case that the purchaser is a merchant. If the purchaser does not have a court of jurisdiction in the Federal Republic of Germany or if he moves his domicile out of Germany after conclusion of the contract, devolo's court of jurisdiction applies. This is also applicable if the purchaser's domicile is not known at the time of institution of proceedings.

g) The law of the Federal Republic of Germany is applicable. The UN commercial law does not apply to dealings between devolo and the purchaser.

Index

C
CE declaration 6
Control lamps 19
D
Default WLAN key 20, 48, 55
devolo dLAN AVpro manager 23, 69
DHCP server 33
Disposal of old devices 72
dLAN AVpro network 65
dLAN encryption 35
dLAN password 35
E
Encryption button 65
Enterprise Mode 48
Enterprise mode 53
I
Important safety instructions 71
IP address 33
L
LAN (Network connection) 21
M
MAC address 46
Management VLAN 34
Multi SSID 43
P
Package contents 18
R
RADIUS server 42
Reset 21
S
Security ID 20
Software installation 23
SSID 43
System requirements 18
T
tagged 59
Time server 36
U
untagged 59
V
VLAN 55
VLAN ID 34, 57
VLAN port 58
W
Warranty 72
WEP 47, 53
Wi-Fi Protected Setup (WPS) 20, 48
WLAN antenna 22
WLAN client 50
WLAN filter 44
WLAN ON/OFF button 20
WLAN time control 41
WPA 47, 53
WPA2 47, 53